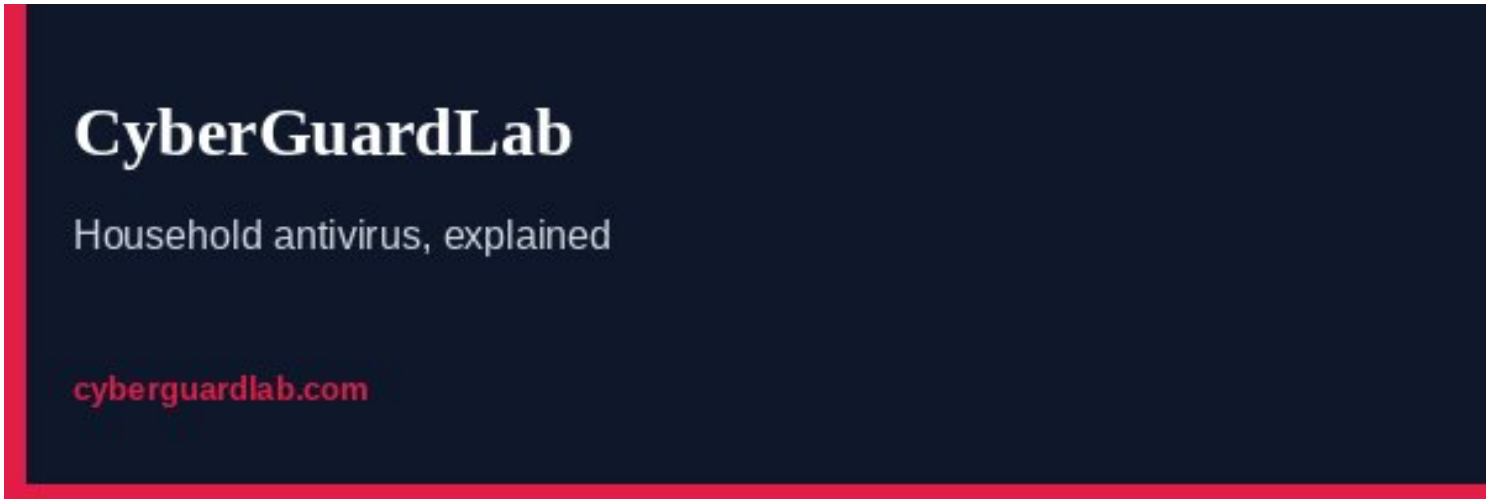
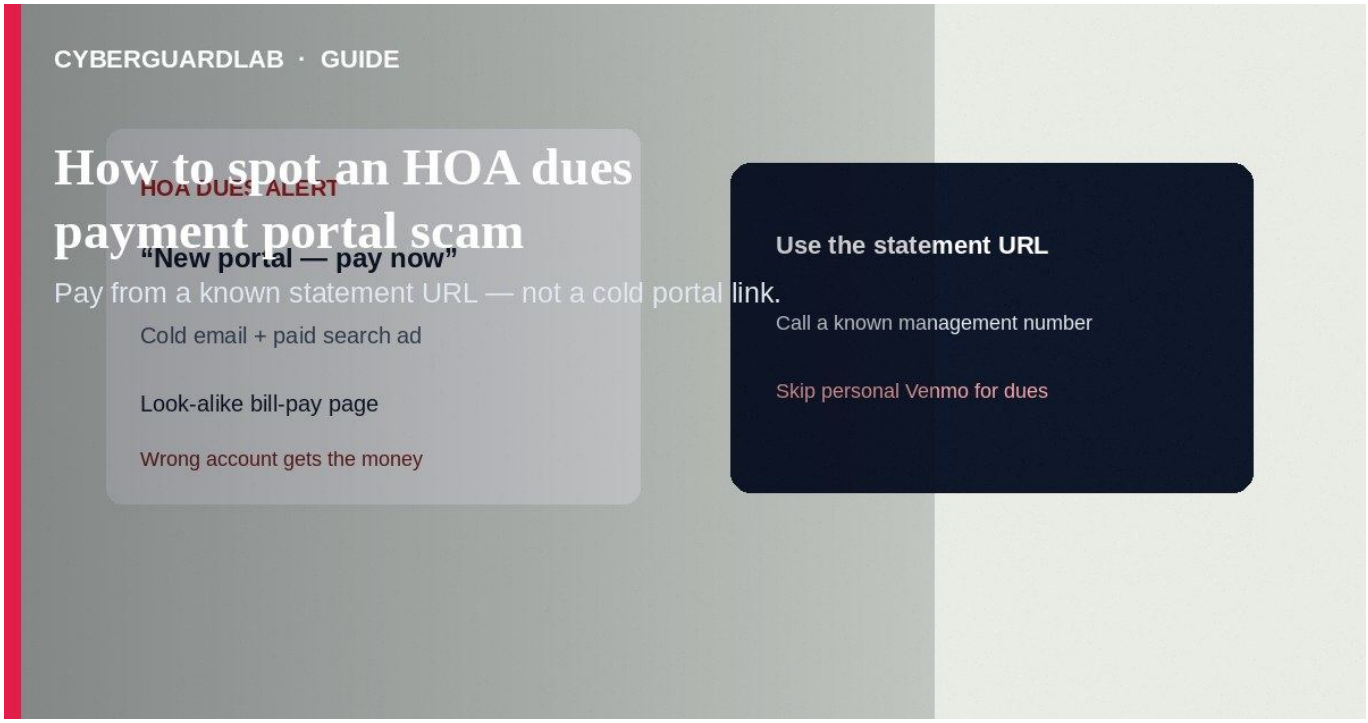


How to spot an HOA dues payment portal scam

https://cyberguardlab.com/blog/hoa-dues-payment-portal-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.



An HOA dues payment portal scam uses a fake management email, search ad, or cloned "resident portal" so you pay assessments to the wrong place-or hand over bank login details. Pay only through the portal or remittance details printed on a statement you already trust, or a URL your management company confirmed out-of-band. This guide is HOA / condo association bill-pay impersonation-not utility shutoff scripts alone, and not general phishing without the dues angle.

What this scam looks like

Messages claim "dues past due-pay in the new portal," "board updated the bank account-wire today," "special assessment: click to avoid a lien," or "your HOA app needs re-login." Search ads for "[your HOA name] pay dues" may open a third-party look-alike that adds surprise fees or never forwards the payment. Some pages harvest routing numbers, portal passwords, or driver's license uploads "for verification."

Legitimate vs scam cues

Cue | Likely legitimate | Likely scam

How you found the portal | URL/app from a prior statement, welcome packet, or management letter | Cold email link or top paid search ad you clicked in a hurry

Payment change | Written notice on letterhead + confirmation via a phone number you already had | "New ACH only" with urgency; wire/gift card/crypto

Fees | Known portal convenience fee disclosed by your association | Unexpected "delivery" or subscription add-ons on an unfamiliar site

Tone | Matches past HOA notices; allows normal grace periods | Lien/foreclosure threats in hours; "board emergency"

Login | Same portal domain you used last quarter | New domain asking for bank credentials or full SSN to "unlock dues"

What to do before you pay

* Open last month's HOA statement or welcome packet. Use the printed portal URL, coupon, or lockbox address-do not trust a new link in email alone.
* If search is your only option, scroll past paid ads. Prefer typing a known management-company domain. FTC guidance on bill-pay impersonators: check the bill, not the ad.
* Any "new bank account / new portal" instruction: call the management company or board treasurer using a number from an old statement or the community website you bookmarked-not the number in the suspicious email.
* Prefer a credit card when the real portal offers one; cards usually give stronger dispute rights than ACH or wire if something goes wrong.
* Turn on MFA on the real resident portal if available; use a unique password (password manager is fine).
* If you already paid the wrong site: contact your bank/card issuer immediately; tell the real HOA so they do not treat you as

delinquent; save screenshots; report at ReportFraud.ftc.gov.
* If you typed portal or bank passwords on a fake page: change them on the real sites from a clean device; watch accounts.
* Scan the PC/phone with Norton or Bitdefender if you opened a shady attachment; or stick with Defender + habits. Optional compares: TotalAV, McAfee, Avast.

Extra caution on "pay the board member's personal Venmo"

Legitimate associations use documented lockboxes, management portals, or association accounts. Personal peer-to-peer apps for dues-especially after a cold email-are a red flag. Confirm with management using a known phone number before sending.

FAQ

Our management company really did change portals-what then?

Expect a mailed or previously used-channel notice. Confirm by calling a number you already had. Do not approve the change only from the announcement email's button.

Is every third-party bill-pay site a scam?

Not automatically-but FTC cases show search ads and look-alike bill-pay pages can add fees or fail to post payment. Your HOA's stated channel wins.

Can I pay by paper check instead?

Often yes, using the remittance address on the statement. That can be safer when a "new portal" feels off.

Someone emailed new wiring instructions for a special assessment.

Treat like business email compromise: out-of-band verify before any wire. Urgent wire + new account is a classic fraud pattern.

Will antivirus stop an HOA portal scam?

It may catch malware on a fake page, but social-engineering payment diversion is mostly stopped by how you navigate and verify-not by a product score.

If you still want a paid suite

HOA bill-pay hygiene is mostly verification, not a product purchase. Buy-nothing is valid. If you still want a paid suite, use only these on-site paid links: Norton (paid link), Bitdefender (paid link), TotalAV (paid link), McAfee (paid link), Avast (paid link).

Sources

* FTC: Searching online - bill pay impersonators (Aug 2026)
* FTC: Pay your bills, not impersonators
* FTC: How to recognize and avoid phishing scams
* CISA: Recognize and report phishing
* FTC: ReportFraud.ftc.gov

Also read

* How to spot a utility shutoff scam
* How to spot a phishing email
* How to spot an apartment rental application scam
* Credit card fraud: first hour
* How to report a scam to the FTC
* How to spot a fake check scam