CyberGuardLab

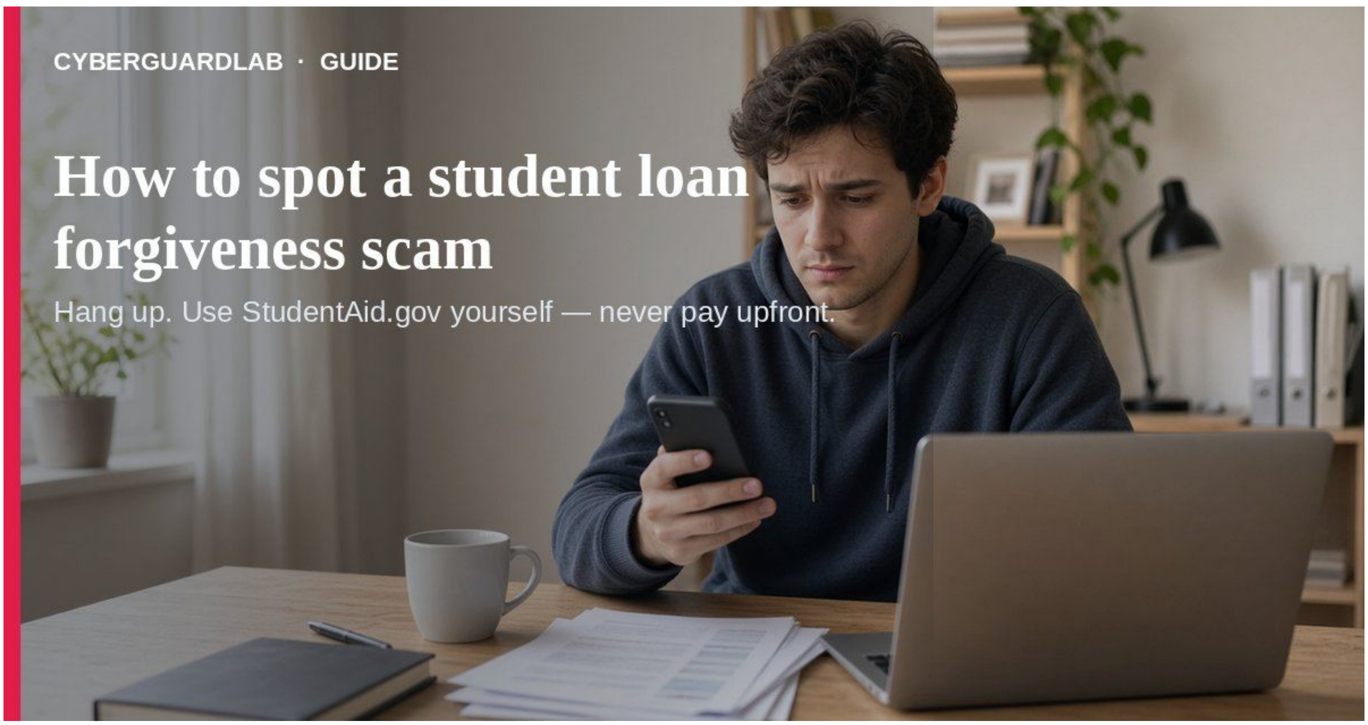
Household antivirus, explained

cyberguardlab.com

How to spot a student loan forgiveness scam

https://cyberguardlab.com/blog/student-loan-forgiveness-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 student loan forgiveness scam is when someone pretends to be from Federal Student Aid (FSA), the Department of Education, or a "special forgiveness program" and rushes you to pay an upfront fee, share your FSA ID / StudentAid.gov login, or sign papers you do not understand. Per the FTC, there is nothing a debt-relief company can do for federal loans that you cannot do yourself for free at StudentAid.gov - and it is illegal for companies to charge you before they help.

This guide is about student loan debt-relief / forgiveness impersonation, not fake IRS refund calls, Social Security suspension threats, or general debt collection scams. You do not need to buy antivirus to hang up and log in at StudentAid.gov yourself.

1. Common student loan forgiveness scam patterns

From FTC guidance on paying for school / avoiding scams and FTC alerts about forgiveness-news scams:

* "You're eligible - act now" cold calls or texts - Someone claims affiliation with FSA or Education, may recite a balance or account number, and says a forgiveness window is closing. FTC: real FSA and your federal servicer will not pressure you that way.
* Upfront fees for "guaranteed" forgiveness - Company demands payment before any help. FTC: it is illegal to charge before helping with student loan debt relief; you may get neither help nor a refund.
* Official-looking seals and logos - Scammers paste Department of Education seals and promise "special access" to consolidations or forgiveness. FTC: there is no special access you cannot get yourself on StudentAid.gov.
* Requests for your FSA ID / StudentAid.gov login - Only scammers say they need your login to "help." FTC: sharing it can cut you off from your servicer or enable identity theft.
* Quick wipe-out promises - Before knowing your situation, they claim they can erase loans or get you into a program most people will not qualify for.

2. What to do when someone contacts you

* Do not pay upfront. Hang up on fee demands for "processing," "enrollment," or "guarantee."
* Do not share your FSA ID or StudentAid.gov password/PIN. Do not read codes from password-reset texts/emails to a caller.
* Verify on official channels. For federal loans, use StudentAid.gov (or StudentAid.gov/repay) or contact your federal loan servicer using a number from your billing statement or the site - not the number in the pitch.
* Private loans: contact your lender directly; federal sites do not manage private loans the same way.
* Ignore "Department of Education seal" on ads. Go to StudentAid.gov yourself in the browser.
* Treat gift cards, wire, crypto, or payment apps as scam rails for a "forgiveness fee" - see also gift card scam.
* Watch for phishing lookalikes. Unexpected "forgiveness" email/text links can be phishing - do not click; type StudentAid.gov yourself.

3. Free help and how to report

* Check eligibility and repayment options on your StudentAid.gov dashboard (FTC: free).
* Call your federal servicer from a verified number if you need plan changes, consolidation questions, or deferment/forbearance options.
* If you already paid a scammer, act quickly with your bank/card issuer; FTC: sooner is better for recovery chances.
* Report at ReportFraud.ftc.gov - walkthrough: how to report a scam to the FTC.
* If someone used your FSA ID or personal data, start recovery at IdentityTheft.gov - report identity theft.

4. Household habits that cut risk (no software purchase required)

* Family rule: StudentAid.gov login is never shared with cold callers, Facebook "helpers," or paid "forgiveness companies."
* Bookmark StudentAid.gov; do not trust search ads that look official.
* When forgiveness is in the news, expect more scam calls - pause, then verify on the site.
* Keep a copy of your latest federal loan statement so fake "account numbers" stand out.
* Teach teens/young adults: free help = StudentAid.gov or your servicer; paid upfront = red flag.

FAQ

How do I spot a student loan forgiveness scam?

Unexpected contact promising fast forgiveness, special access, or requiring an upfront fee or your FSA ID matches FTC scam patterns.

Can a company get me forgiveness I cannot get myself?

FTC: for federal loans, nothing a company can do that you cannot do for free at StudentAid.gov.

Is it legal for a company to charge before helping?

FTC: it is illegal for companies to charge you before they help reduce or eliminate student loan debt.

Is this the same as an IRS or Social Security scam?

Related government-impersonation family, different script. See fake IRS tax refund scam and Social Security scam.

Do I need antivirus to stop this scam?

No. Hang up, use StudentAid.gov, and report. Buy-nothing is valid - see Is Microsoft Defender enough?.

If you still want a paid suite

Spotting a student loan forgiveness scam does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. 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

* Paying for School and Avoiding Scams (FTC)
* Scammers follow the news about student loan forgiveness (FTC)
* StudentAid.gov (Federal Student Aid)
* ReportFraud.ftc.gov (FTC)
* IdentityTheft.gov (FTC)

Also read

* How to spot a phishing email
* How to spot a fake IRS tax refund scam
* How to spot a Social Security scam
* How to spot a gift card scam
* How to spot a fake debt collection scam
* How to report a scam to the FTC
* How to report identity theft at IdentityTheft.gov