U.S. DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Protect Yourself from Student Loan Debt Relief Scams

TIPS IN BRIEF

1. **Protect Your Personal Information and Passwords**
2. **Be Wary of Companies that Promise Student Loan Relief—for a Fee**
3. **Don't Get Hooked by Phishing Scams**
4. **If You Think You've Been a Victim of a Student Loan Debt Relief Scam, Act!**

Fraudsters and cyber criminals prey on student loan borrowers and their desire to pay down or consolidate student loan debt. Don't fall for it!

Your identity stolen. Credit cards and loans taken out in your name. Bank account zeroed out. Credit score ruined. This is what can happen if you fall victim to a student loan debt relief scam!

Dishonest companies and cyber criminals are targeting student loan borrowers, sending unsolicited texts, emails, or calls with promises to help reduce your student loan debt, consolidate your student loans, or eliminate your student loans completely. You may also see their ads pop up on social media. Don't fall for it—these are likely scammers coming after your money, your personal information, or both.

The U.S. Department of Education Office of Inspector General (OIG) encourages you to take these simple steps to avoid falling victim to student loan scammers, and shares actions to take if you think you've been caught in their traps.

FIRST TIP

Protect Your Personal Information and Passwords

Cyber criminals and scammers are coming after your money and your personal information—your date of birth, debit or credit card number, your Social Security number, even your FSA ID. Here are some actions to take to protect yourself.

1. Don't share your FSA ID or other password with anyone—even people who say they work at your alma mater or your student loan servicing company. Remember, you agreed to protect and not to share your FSA ID as a condition of it being issued to you by the Department of Education.
2. Don't store your passwords where other people can see them.
3. Use multifactor authentication/two-step verification where it's available.
4. Use strong passwords.
   - Don't use personal information in your password (like your name or birthday).
   - Avoid using terms that could be socially engineered (like the name of your pet or favorite sports team).
   - Avoid using the same or similar passwords across multiple platforms

SECOND TIP

Be Wary of Companies that Promise Student Loan Relief—for a Fee

It's important that you act cautiously if you receive an unsolicited phone call, text, email, or social media message offering you loan forgiveness or special repayment programs, especially those that pressure you to respond immediately. There are bad actors out there promising to reduce or wipe out your loans entirely in exchange for up-front or monthly fees. Sometimes they are just charging you for what you can do for free by contacting your loan servicer. Other times, they just take the money and run. Follow these steps to avoid falling victim to debt relief scams.

1. Get the facts on Federal student loan repayment and forgiveness directly from the source: the U.S. Department of Education Federal Student Aid office.
2. Don't give out your personal information over the phone or email unless you initiated the contact.
3. Remember, if a company asks you to pay a fee for any Federal student loan services, don't give them anything!
4. Learn more about student loan scams and how to avoid them from the U.S. Department of Education's Federal Student Aid office.

THIRD TIP

Don't Get Hooked by Phishing Scams

Cyber criminals lure student borrowers into their traps through phishing. Phishing scams are emails, texts, phone calls, or DMs trying to get your personal information. These messages may look like they're from your bank, alma mater, student loan servicer, or even the U.S. Department of Education. They can be very convincing and will often rely on emotion or urgency in the hopes of tricking you into thinking it's legitimate. Keep the following things in mind and avoid getting hooked.

1. Beware of emails from vague sender names like "Student Loan Department" or "Financial Aid Office." If no additional information is provided (like the name of a school or company) it's likely a scam.
2. Be suspicious of any unsolicited email, text, or call that asks for your personal information.
3. Don't click on links or attachments embedded in emails from unknown sources. Hover your mouse over links to see where they are actually going.
4. Look for misspellings in the email address, body of the message, or in links. A common tactic phishing scammers employ is to use addresses that are almost—but not quite—identical to legitimate ones

FOURTH TIP

If You Think You've Been a Victim of a Student Loan Scam, Act Immediately!

If you suspect that your personal information has been stolen as a result of a student loan debt relief scam, take action quickly! Here are some helpful tips aimed at protecting your identity and your money!

1. Contact Federal Student Aid and your loan servicer to let them know about the situation.
2. Contact the credit reporting agencies and freeze your account so nobody else can open new credit accounts in your name. You'll find tips and credit agency contact information on the identitytheft.gov website.
3. If you receive an email, text, or call that you believe is a scam, let us know! Contact the OIG Hotline to share what you received!
4. Stay on top of student loan scams by visiting the Federal Student Aid, the Consumer Financial Protection Bureau, and the Federal Trade Commission

Remember to Remain Vigilant

We know it's hard with everything you have going on, but we strongly encourage you to take the above actions to better protect yourself from student loan cyber criminals and phishing scammers. We also encourage you to exercise those well-known rules of the technology road: keep your devices safe and updated, avoid doing financial transactions (particularly those involving your student loans) over public Wi-Fi or on shared computers, and keep your eye on your accounts for any unusual activity. By following these simple practices you'll be better positioned to protect yourself and your personal information!

U.S. DEPARTMENT OF EDUCATION, OFFICE OF INSPECTOR GENERAL

HOTLINE

OIGHOTLINE.ED.GOV

The U.S. Department of Education Office of Inspector General is responsible for identifying fraud, waste, abuse, and other criminal activity involving Federal education programs, operations, and funding. For more information about us, visit our website at oig.ed.gov, and follow us on Facebook, Twitter/X, and LinkedIn.