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 college graduates, 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—they are likely scammers coming after your money, your personal information, and your identity.

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

### Protect Your Personal Information and Passwords

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, or 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.

- 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 servicer 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.
- Don’t store your passwords where other people can see them.
- 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.

Don’t give out your personal information over the phone or email unless you initiated the contact.

Be suspicious of any unsolicited email, text, or call that asks for your personal information.

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.

Be suspicious of any unsolicited email, text, or call that asks for your personal information.

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.

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.

Don’t use personal information in your password (like your name or birthday).

Don’t give out your personal information over the phone or email unless you initiated the contact.

Get the facts on Federal student loan repayment, consolidation, and forgiveness directly from the source: the U.S. Department of Education Federal Student Aid office.

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

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 college graduates, 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—they are likely scammers coming after your money, your personal information, and your identity.

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

### Protect Yourself from Student Loan Debt Relief Scams

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.

- 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 servicer 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.
- Don’t store your passwords where other people can see them.
- 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.

### 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, or 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.

- 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.
- Be suspicious of any unsolicited email, text, or call that asks for your personal information.
- 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.
- 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.

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!