Protect Yourself from Cyber Scammers and Identity Thieves!

Cyber criminals and identity thieves prey on college students, looking to steal your personal information, your money, or both! The impact of their scams can be severe—your identity stolen, credit cards and loans taken out in your name, bank account zeroed out. That's why the U.S. Department of Education Office of Inspector General (OIG) encourages you to take these simple steps to protect yourself and your personal information.

1 Protect your personal info—including your FSA ID!

- Don't share your FSA ID or other password with anyone, not even your school representative! 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.
- Always use strong, unique passwords.

2 Don't get hooked by phishing scams!

Phishing scams are emails, texts, phone calls, or DMs trying to get your personal information, including your school log-in credentials!

- Be suspicious of any unsolicited email, text, or call that asks for personal information or school ID.
- If you receive an unsolicited message like this or about your student loan, contact your school's financial aid office.

3 Think you've been hacked? Act!

If you suspect that your personal information has been stolen, take action quickly!

- Contact your loan servicer and let them know about the situation.
- Contact the credit reporting agencies and freeze your account so nobody else can open new credit.
- Contact the OIG Hotline and share a copy of the email, text, or phone number related to the call you received!

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 www.ed.gov/oig, and follow us on Twitter and Facebook.