U.S. DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Protect Yourself from Cyber Scammers and Identity Thieves!

TIPS IN BRIEF

1. **Protect Your Personal Information and Passwords**
2. **Don't get hooked by phishing scams!**
3. **Think you've been hacked? Act!**

As a college student, you live on your devices—like your phone and laptop—and rely on them for your social and scholastic lives. Cyber criminals and identity thieves know that too, which is why so many prey on college students, looking to steal your personal information, your money, or both!

The impact of these student-centered 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 avoid falling victim to student-centered scammers, and shares what to do if you think you've been caught in their traps!

FIRST TIP

Protect your personal information and passwords—including your FSA ID!

Cyber criminals and identity thieves target college students because they see you as easy prey: you're busy with school, you're online a lot, and you're not thinking about being scammed. That's why they think they can con you into handing over your debit card number, your Social Security number, even your FSA ID! Prove them wrong by taking a few simple actions to protect yourself.

1. 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.

2. 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.
3. Use multifactor authentication or two-step verification where it's available.

SECOND TIP

Don't get hooked by phishing scams!

Cyber criminals and identity thieves lure college students into their traps through phishing. Phishing scams are emails, texts, phone calls, or DMs trying to get your personal information, including your school log-in credentials! They could be offering help paying for college, or paying down or consolidating your student loan. They could say you've won a scholarship that you never applied for! Phishing scams can be very convincing and will often rely on emotion or urgency in the hopes of tricking you into thinking they're legitimate. Phishing scams may appear to be from your bank, school, or even a classmate, friend, or relative. Keep the following things in mind and avoid getting hooked.

1. No legitimate organization will award an unsolicited scholarship through email, text, or phone, and ask you for your bank or school account information to wire the funds to you. Stay alert—it's likely a fraud!
2. No one but you needs to access your FSA account, so if a company or person is promising to help you pay for college or help with your student loan but needs access to your account to do it, don't fall for it—it's likely a scam!
3. Be suspicious of any unsolicited email, text, or call that asks for personal information like your birthday, Social Security number, or school ID.
4. If you receive an unsolicited email, text, or call that involves your student loan in any way, contact your school's financial aid office immediately. It could be a scam and you may not be the only one who received it!
5. 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.
6. Look for misspellings in the email address, in the body of the message, and in links. A common tactic phishing scammers employ is to use addresses that are almost—but not quite—identical to legitimate ones.

THIRD TIP

Think you've been hacked? Act!

If you suspect that your personal information has been stolen or you're the victim of other student-centered crime, take action quickly!

1. Contact your loan servicer and 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 or text that you believe is a scam, let us know! Contact the OIG Hotline and be sure to share a copy of the email, text, or phone number related to the call you received!
4. Keep an eye on the website of your school's financial aid office as they may provide information on student loan and other scams targeting their students. And you can stay on top of student-centered scams by visiting Federal Student Aid, the Consumer Financial Protection Bureau, and the Federal Trade Commission

We Know You'll Keep Scrolling... Do it Safely

We know it's hard with everything you have going on at school, but we strongly encourage you to take the above actions to protect yourself from cyber criminals and identity thieves. Also remember to exercise these well-known rules: (1) avoid using public Wi-Fi or public kiosks, (2) never leave your devices unattended in public spaces, (3) lock your screen or device when unattended, and (4) keep your devices up to date. 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.