BANK OF AMERICA

Students: How to spot 6 common scams

As a high school or college student, you have many responsibilities such as studying for exams, holding down a part-time job and handling at least some of your own finances. While you're doing all this, con artists may also be trying to separate you from your cash. Cybercriminals know students often have hectic schedules and may be new to money management, making you an ideal target.

The good news? You can protect your financial and personal information by familiarizing yourself with the most prevalent scam tactics and how to spot them.

Here's what you need to know about six of the top scams that target students.

1 Fake apartment listings

How it works

You see an online listing for what seems to be an ideal apartment. The landlord or agent isn't able to show you the place, but you can secure it immediately if you mail or wire a deposit — only to find out later that the ad was phony and your money is gone.

Action to take

Do an Internet search on the apartment's address and any contact names you come across. You may find the legitimate listing for that apartment or learn that others had been scammed in the same way. If the apartment is in your area, always view it in person. In all cases, never send money without first confirming that a listing is legitimate.

Red flags

Be wary if the listing sounds too good to be true, or if you can't see the unit in person. Other bad signs: There are typos in the listing, a vague description of the apartment and/or no formal rental application or tenant.

2 Bogus scholarships and grants

How it works

You receive a call or email saying you earned a grant or scholarship. You're asked to make an upfront payment for processing or related services, but the scholarship or grant money never materializes.

Action to take

Contact your school to see if anyone there can help to confirm the legitimacy of the award. In addition, research the organization giving the scholarship or grant to see what information you can find out. Under no circumstances should you be required to send money for a scholarship or grant.

Red flags

Be suspicious if you never applied for the grant or scholarship. Also, stay on high alert if you're told the award is a "sure thing," that it's only available for a limited time, or that the awarding organization is a newly formed company.

3 Unpaid tuition claims

How it works

A person claiming to be a representative of your college calls to say that your tuition payment is late and that you'll be dropped from all classes unless you pay immediately over the phone.

Action to take

End the call, then contact your school's financial aid office through a verified phone number from the school's official website or correspondence. Report the incident to your school.

Red flags

If you're up to date on your tuition payments or if the caller pressures you to pay immediately, these are major warning signs.

4 Counterfeit check cashing

How it works

You receive a cashier's check from someone you don't know, such as a shopper who wants an item you're selling online. The amount is for more than is owed, so you're asked to deposit the check and return the extra funds. Yet, the check is counterfeit, and by the time you and your bank discover that, you've already sent money to the scammer.

Action to take

Never return the amount overpaid until you have confirmation that the check has fully cleared. If the con artist contacted you via a website, notify that site.

Red flags

Be wary if you're given a check that is larger than the amount due, then asked to return funds to the person who paid you. Here's what con artists capitalize on: While the deposited money may appear to be available in your account, a check isn't valid until your bank gets the money from the issuing bank.

5 Improper employment offer schemes

How it works

You see a job posting that promises great benefits such as flexible hours and above-average pay. But you have to pay an upfront fee to move forward in the interview process or to secure the role. In some cases, the application asks for personal information, such as your Social Security number, which the cybercriminal can then use without your knowledge or permission.

Action to take

Cut off contact with any firms that ask you to pay an advance fee for a job. If you sent money as a fee, report the scam to the website where the listing was posted.

Red flags

If you're told you need to pay an application fee, the posting is likely a scam. It's also a bad sign if the so-called employer makes an offer without asking you to interview.

6 Suspect sweepstakes and giveaways

How it works

You receive a call, email or social media message that is purportedly from a company that distributes sweepstakes or lottery winnings notifying you that you've won a contest, but you need to pay a processing fee or taxes to claim the prize. In some cases, scammers will ask for your bank or credit card information, saying they will directly deposit the winnings into your financial accounts.

Action to take

If you feel that you perhaps won a legitimate prize, look up the official website of the group contacting you for information on how to proceed.

Red flags

As with other scams, proceed with caution if you didn't enter any such sweepstakes, you're asked for financial or personal information, or to pay a fee.

Regardless of the scam you may be facing, exercising caution is the key to protecting yourself. If you do fall victim to one of these tactics, don't be embarrassed to take action. By reporting the incident, you can help yourself and prevent others from falling for the same scam.

How to react if you suspect you've been targeted

- **Act quickly** after an incident, as it can help minimize damages.
- **Change all passwords** that may have been compromised.
- **Call the police** and file reports with the relevant local authorities. Many state attorney general websites have detailed information on the latest scams, and online forms to file a consumer complaint.
- **File reports** with the Federal Trade Commission and the FBI's Internet Crime Complaint Center.
- **Document everything** about the incident. The more information you have, the better armed you will be to assist an investigation by law enforcement officials.
- **Alert your bank** about the scam. Although the recovery of lost funds isn't possible in most cases, your bank may be able to use the information to warn other clients.

BANK OF AMERICA