Advice and Tips to Avoid Being Scammed

College students are a vulnerable population for scammers. There are scams that have been created specifically to target the college population. Scammers want you to make decisions in a hurry, and they might even threaten you once they have your money. Before you give up your money or personal information to anyone, slow down, check out the story, do an online search, consult an expert, or discuss it with a family member or friend.

Below are some tips and warning signs to avoid being victimized by a scam:

1. To avoid scam attempts – Never give out your personal information (name, address, date of birth, banking account information, user name, password, or social security number) to anyone unless you are 100% sure of the entity being a legitimate organization or financial institution. Make sure you always log into a website by going directly to the organization's URL, and always check the address bar to make sure you have not been redirected to a copycat site as part of a fraud. Whenever in doubt, contact the company directly, and if something sounds too good to be true, it probably is.
2. Free Public Wi-Fi – Whenever using an unsecured connection, never login to sensitive sites, like your bank account. Additionally, using password protection software and encryption can also make your activities harder to track.
3. Behavior blackmail – Always be mindful of your behavior and surroundings. Make sure you do not upload sensitive pictures or videos to social media sites that may be a bit reckless, embarrassing, or harmful to your reputation. Scam artists prey on vulnerable situations; they access this information and use it as a tactic for blackmailing students to extort money.
4. Fake credit card or financial scams – Be aware of credit card or financial loan solicitations that are received through email or phone calls. Scammers are using these methods as a tactic to gain access to your valuable personal information. Never respond to any phone or email solicitation attempts for these offers. If the offer sounds too good to be true, it most likely is a fraud. If you are looking for loans to pay educational expenses, consult the University of Louisville's Financial Aid Office or reputable loan providers. Never give out your personal information to any unknown source.
5. Advance fee scams – If you are presented with an offer that requires you to pay an upfront fee to receive funds or services in return, do not respond to the email or immediately discontinue the phone call. Solicitations for upfront fees are most likely coming from a fraudster; do not provide any upfront payment or personal information.
6. Never deposit a check and wire money back – By law, banks must make funds from deposited checks available within days, uncovering a

fake check can sometimes take weeks. If a check you deposit turns out to be a fake, you are responsible for repaying the bank.

7. Spot imposters – Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a company you do business with on regular basis. Never send money or give out personal information in response to an unexpected request whether it comes as a text, a phone call, or an email.
8. Hang up on robocalls – If you answer the phone and hear a recorded sales pitch, hang up and report it to the Federal Trade Commission (FTC) (https://www.ftccomplaintassistant.gov). These calls are illegal, and often the products are bogus. Do not press 1 to speak to a person or to be taken off the list. That could lead to more calls.
9. Be skeptical about free trial offers – Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. Always review your monthly bank statement for charges you do not recognize.
10. Sign up for free scam alerts from the FTC at ftc.gov/scams. Get the latest tips and advice about scams sent right to your inbox.