

A **Scammer** is a person who commits fraud with a dishonest plan to gain currency and/or access to sensitive information from unknowing participants.

TOP 3 Scams to Avoid

1. **Emails from Abroad** -- These scams are often called Nigeria Scams because many of them originated from Nigeria. The scams involve an email from someone overseas offering you a large amount of cash – but before giving you the cash, they want help transferring the cash out of their country.
2. **Lottery Scams** -- The scams often involve the scammer telling the victim that they have won large amounts from a lottery. However, before the winners can get the money, they need to pay a fee.
3. **Crypto Rip-Offs** -- Many cryptocurrencies have hit the financial market in the last two years after Bitcoin's big success.

HOW TO AVOID SCAMS

1. **Keep your personal information to yourself.** Because some of the most common scams attempt to gain access to your personal information, one of the easiest ways to avoid scams is to protect that personal information. Keep passwords, account numbers, and sensitive paperwork in a safe place. Do not keep this information on your phone where it can be found.
2. **Conduct online searches.** When you get mailings that ask for money or information, follow-up and do some research about the company or person asking for the information. Never assume a solicitation is legitimate. Try doing the following, which should help you avoid scams:
3. **Call people back using genuine phone numbers.** In today's world, it is easy for scammers to manipulate caller IDs and phone numbers. If you get a phone call from someone, ask them for their name and the company they work for, so you can call them back. Once you get off the phone, look up that company's information online and only call back legitimate numbers found on reputable websites.
4. **Avoid paying any money upfront.** A lot of scammers will request money in exchange for a promise to send you more in return. Scammers will usually tell you that you have won a prize and that you need to pay taxes or fees in order to collect the prize. They might also ask you to pay in advance for a job, debt relief, or for loan assistance.
5. **Think about the payment method being requested.** Scammers will request money from specific sources in order to avoid detection. Most scammers will request cash, money wires (e.g., Western Union), or prepaid credit cards (e.g., Vanilla). These payment methods are difficult to track and nearly impossible to reverse. No legitimate company will ask you to pay using these methods.
6. **Consult people you trust.** Before you give out your personal information or money, talk to someone you trust about what is going on. This could be friends, family, or professionals (e.g., a lawyer, a bank employee, or a government employee). Tell them about the solicitation and ask whether they have seen anything similar before.
7. **Read cancellation policies.** A lot of free trials will automatically turn into large monthly charges, and some trials will not even allow you to cancel for a certain period. Before you accept a free trial for things like television channels, weight loss supplements, or anything else, make sure you look over the company's cancellation policy.
8. **Avoid depositing checks from people you don't know.** A lot of scammers will offer you a large amount of money by check if you send a smaller amount of money in cash or through a wire. However, the check you receive will usually be fake. While a bank may accept the check upfront, it will always be uncovered as fake at some point. When that time comes, it will be your responsibility to repay the bank.

Unfortunately, scams occur regularly and can happen to anyone, but by staying aware, protecting your sensitive information and educating yourself about current/new scams can help prevent you from being a victim!

[Learn more at hcfcu.com/fraud-center](https://www.hcfcu.com/fraud-center) and [download available information sheets.](#)