RED FLAGS: THINGS TO WATCH FOR

Learn to recognize the signs that something is amiss.

Wire transfer. Many scams involve a request to wire money electronically using a money transfer service, like MoneyGram and Western Union, or using cryptocurrency, such as Bitcoin. Remember that sending a transfer through these services is like sending cash—once the amount is picked up, it's almost impossible to get your money back.

Overpayment. When you're selling something—especially online—be wary of how you get paid. A fraudster may send you a counterfeit cashier's, personal or corporate cheque in an amount in excess of what they owe. You'll be asked to deposit the cheque and wire the excess funds immediately back to them. Once your bank realizes the cheque is a fake, you'll be on the hook for the money withdrawn.

Spelling mistakes. Be skeptical of emails, messages or websites that contain misspelled common words; grammar errors that make it difficult to read or expressions that are used incorrectly. Email and web addresses should also be examined closely to see if there are subtle mistakes or differences.

Personal information request. Fraudsters may ask potential victims to provide more personal or financial information than is required for the transaction or discussion. Be suspicious if someone asks for copies of your passport, driver's licence and social insurance number, or birth date, especially if you don't know the requestor.

Unsolicited calls. You might get a call from someone claiming that you have a virus on your computer, you owe taxes or there has been fraudulent activity in your bank accounts. Know that legitimate organizations will not call you directly. Hang up and call the organization yourself using the number from a trustworthy source, such as the phone book, their website, or even invoices and account statements.

Unsolicited friend requests on social media. Don't accept friend requests from people you don't know until you review their profile or ask your real-life friends if they know them. Does their profile look fairly empty or have posts that are very generic? Do they seem to be promising more than friendship? These are some red flags that point to a scam. Delete that request and block future ones.

Astounding mail offers. You received a game card in the mail. It guarantees you will or have already won. Prizes might range from cars to trips. If you have not entered a contest, throw that card away. It's probably a scam!

It's just too good to be true. Everybody loves a great deal. But shocking offers, unbelievable discounts and unreal rates may signal that the offer isn't quite what it seems. Cheap prices usually equal cheap products, or counterfeit goods. Free offers may require providing your credit card for shipping. Small tactics like these can lead to big profits for scammers.