Authorised Push Payment Scams also known as APP Scams are when you are persuaded into sending money to a criminal. With banking systems getting more and more secure, fraudsters now try to get you to send them your money by pretending to be someone you trust. They can be tough to spot, but if we know what to look out for we can stop fraudsters in their tracks.

Someone may contact you by phone, by text message or by e-mail, pretending to be someone you would trust. It could be your bank, utilities provider, the CRA or another company you already do business with.

They might say your account is under attack and you must move your money to a safe account to protect it. They might say your last payment didn't go through and you need to update your bank details. They may even claim to be from the CRA reaching out to tell you that you owe back taxes that must be paid immediately before they issue a warrant for your arrest.

In short, they want to cause you concern and instil panic, hoping that you will agree to transfer your money before thinking about what you're doing.

If this happens, there are three easy steps to keep in mind:

1. If someone calls you and asks you to move your money, don't, even if it's to another account you already hold.

2. Remember, we will never ask you to transfer funds to a safe account or another bank. If you receive a call asking you to do this, hang up the phone, wait at least 15 seconds to ensure the line is disconnected, then call the number on the back of your HSBC Debit or Credit Card.

3. Call us, at any time. If you think you have been a victim of this fraud, our team may be able to help.

By educating ourselves and others about fraud, we can stop fraudsters together by staying alert.