

E-Transfer Interception

E-transfer interception can occur when a fraudster gains unauthorized access to an e-transfer recipient's email account or phone number. By gaining this access, the fraudster can use the deposit link to redirect funds into a different account, if they are able to answer the security question.

How to protect yourself:

Register for Autodeposit

Autodeposit will allow you to have money automatically deposited without answering a security question. This makes it more difficult for fraudsters to intercept the transfer.



Secure Your Questions

Choose a security question with an answer that is difficult to guess or discover. Communicate the answer to the recipient in-person or by phone call. Never share your security answer through email, text or social media. Also, do not include it in the e-transfer message area.



Beware of Unexpected Transfers

If you receive a deposit notification that you were not expecting, contact the sender through a different channel to confirm the transfer is real. Do not click on any links in e-Transfer notifications from a sender you don't recognize.



Be Careful with Social Media

Always be careful what information you share on social media. Fraudsters visit social media pages to find relevant information about you.

