Dated: February 3, 2020

Advisory: Intercepted e-Transfers

We have detected a recent spike in an attack vector called "*Intercepted e-Transfers*".

What is an Intercepted e-Transfer you wonder?

This occurs when a legitimate customer sends an e-Transfer to someone they know. Criminals seize the opportunity to deposit the funds to a mule account before the intended recipient has the chance. The interception is not caused by a vulnerability in *MemberDirect* or the *Interac* e-Transfer product, but rather because the recipient's email account was accessed by a criminal. Once in that account, criminals can "see" the notification from *Interac* and use the deposit link to redirect funds into a different account by answering the security question.

Here are some tips to help you protect yourself. You should:

- Not communicate the answer to the security question via email. Call and/or text the recipient with the password.
- Select a question and answer that is not easy for a third party to guess. If the notification is intercepted, it will be harder for a criminal to answer and steal the funds.
- Be cautious not to click on any phishing links and ensure that you are only transacting with trusted websites, vendors, and people.
- Immediately notify Eagle River Credit Union if you sense anything suspicious about your transaction.
- Register for Auto Deposit. This will make sending money on the e-Transfer service more secure.

Interac announced that they will begin scoring, alerting, and reporting on suspicious e-Transfers sent to potentially compromised email accounts to proactively prevent being intercepted by an unintended recipient.

8 Branch Rd
PO Box 29
L'Anse au Loup, NL A0K 3L0

Tel: (709) 927-5524
Fax: (709) 927-5759
erinfo@ercu.ca
www.eagleriverecu.com