SENIOR EXECUTIVE IMPERSONATION SCAM

After hacking into a senior executive's email account, a scammer contacts an employee who is authorized to make international wire transfers for the business. Using the executive's email address, the scammer asks the employee to transfer money to a foreign account for an emergency or an important acquisition. There are usually a number of emails back and forth, but the hacker demands that the employee keep everything under wraps

DO YOU THINK YOUR BUSINESS HAS FALLEN VICTIM TO FRAUD?

- Contact your financial institution and the police immediately

- Report all fraud to the Canadian Anti-Fraud Centre at **www.antifraudcentre-centreantifraude.ca**

BEST PRACTICES

1. **Train your staff**

All staff involved in the business's financial activities must be taught about fraud schemes and receive training on fraud prevention procedures.

2. **Institute a strict procedure for wire transfers**

Your wire transfer procedure should be spelled out in writing and known only to staff who complete transfers.

- Identify which staff members are authorized to carry out wire transfers.
  - —Establish a process for confirming wire transfer requests.
  - —Determine the maximum amount each staff member may transfer.
  - —Require supervisor authorization for transfers exceeding the authorized limit.
- Systematically verify officer requests not made in accordance with the procedure directly with the officer using another means of communication, especially when strict confidentiality is required.
- Regularly verify that the staff in question understand the procedure and are following it.