

Special Notice: Fraudulent Employment Offers

Recently at the Ross Memorial Hospital a certain persons and/or agency have been sending fraudulent offers of employment on behalf of Ross Memorial Hospital to healthcare professionals, primarily in India. While the sending of fraudulent offers of employment has not involved Haliburton Highlands Health Services we felt that it was important to communicate regarding this employment scam.

The fraudulent offers of employment were sent by persons or agencies purporting to be the Ross Memorial Hospital. They were also illegitimately using Ross Memorial Hospital logo and pretending to be from the Human Resources department.

Please note our Ross Memorial Hospital and Haliburton Highlands Health Services do not and would not offer an employment contract in exchange for payment.

The fraudulent employment offer was from admin@r-m-h.org, and/or contained the telephone number 1-646-844-8464.

To view current Haliburton Highlands Health Services vacancies, please go to

<https://www.hhhs.ca/careers>

Thank you

HHHS Staff,

Recently there have been several fraudulent offers of employment on behalf of Ross Memorial Hospital to healthcare professionals, primarily in India. Haliburton Highlands Health Services has not been a target of these fraudulent employment offers thus far. These offers are an attempt to solicit and collect personal identifying information. You should be aware of these attempts to obtain personal identifying information as it is the primary tool for hackers.

Here are some ideas to help protect you.

1. Use and keep up-to-date security software on personal computers.
2. Learn to identify spam and fraudulent inquires.
3. Use a strong password on all your computing devices.
4. Monitor and review your credit scores.
5. Investigate the use of credit alerts offered by TransUnion and Equifax credit bureaus which will notify you if a request has been made for a new credit product. There may be a cost associated with this offered feature.
6. Purchase from reputable online websites only.
7. Watch for common signs your identity maybe compromised:
 - a. False information appearing on credit reports.
 - b. Missing bills or bills mailed to you.
 - c. Getting new credit cards you didn't apply for.
 - d. Being denied credit approval or only being offered higher than expect interest rates when there is no reason.
 - e. Receiving calls from collections or notice of overdue bills you didn't authorize.
8. Be cautious on using public open wi-fi on unsecured networks. If you are using these networks use a Virtual Private Networks (VPN) to protect your connection.

If you should have any questions around identity thief, if you have been sent questionable unsolicited email or unsure of an internet website validity please contact the IT helpdesk (helpdesk@hhhs.ca) before opening emails, responding to emails or accessing questionable internet websites.