Take Precautions Against Cybersecurity Threats

In this time of moving our practices online we need to be vigilant regarding online scams and other cybersecurity threats. The CAMFT board has already been the target of sophisticated email scams that looked very realistic.

Insurance provider HIROC recently issued the following alert regarding cyber threats to health care providers' information security, client confidentiality and privacy:

Healthcare organizations have, unfortunately, become a popular target for scammers and fraudsters during the COVID-19 pandemic. A number of international law enforcement agencies (including the FBI and CSIS), financial institutions, and cybersecurity centres have recently issued warnings related to an increased risk and incidence of social engineering scams directed at the healthcare sector.

Here are a few examples of social engineering **scams**:

- Criminals impersonating colleagues, friends, employees or vendors requesting changes to deposit bank accounts or requesting emergency financial help
- Fake COVID-19-themed emails coercing staff to click on malicious links that then download malware or ransomware
- Emails requesting users to log into their banking website to update information. These emails contain links to malicious websites that have been set up to look like legitimate sites (e.g. financial institutions such as banks and credit unions, and vendor websites)

With this increase in risk, it is important that we all develop good security habits and remain vigilant and suspicious of all emails.

Cybercriminals have become very sophisticated and are using "spoofing" functionalities that make **fraudulent emails** look virtually identical to legitimate emails. They often will create "new" email address that are in your name to send to your contacts. Always check to see who the email is actually from.

HIROC advises:

- Scrutinize emails for unusual behaviour, language, and circumstances
- Verify the validity of email requests before taking any actions, including, but not necessarily limited to the following:
    -

- Changing banking details
- Processing urgent payments or online banking
- Out of the ordinary requests for emergency help
- Logging into websites
- Clicking links
- Opening unverified attachments

HIROC recommends that we all adopt robust verification processes and practices, such as secondary sign-off on payment detail changes, and phone verification using known contact numbers.

Change your password at least once a year. Make your passwords complicated using numbers, letter, capitalization and special characters (!@#$%?:;). Keep a list of all your passwords on paper in a safe place at home or work. Write down beside the password the last time you changed it.

Does Your Insurance Cover Cybersecurity Threats?

If you are **insured with McFarlan Rowlands** through the CAMFT your policy covers E- Counseling automatically.

Cyber Liability (Digital security & Privacy Liability, Data Loss, Hacking, ransomware, cyber-crime) requires its own policy. Please contact McFarlan Rowlands directly to receive a quote for coverage on Cyber Liability at 877-679-5440 or mentalhealth@mcfr.ca.

If you are **insured elsewhere**, take time to review the terms of your practice insurance. Particularly if you are new to electronic practice, contact the brokerage or professional association you purchased your insurance from to find out if you have any vulnerabilities in your coverage.

The above email was partially created with resource information from CRPO.