PROTECTING YOUR DIGITAL HEALTH

Canadian nuclear utilities, Canadian Nuclear Laboratories and the Canadian Nuclear Safety Commission are viewed as world leaders in the area of cybersecurity. Cyber security measures in nuclear plants include processes, procedures and technical measures. Combined, these steps can be effective in combatting cyber threats. COG supports these efforts through information sharing, events and a peer group focussed on cybersecurity best practices.

With the Canadian Centre for Cyber Security and others within the Canadian IT and cybersecurity communities reporting an increase in cyber-attacks on remote workers since the COVID-19 pandemic forced many to transition to their home offices, these protections are being put to the test. The attacks are designed to take over computers and mobile devices, defraud victims of funds and steal data.

Like our members, COG is continually upgrading and evolving with technology to ensure a safe and secure online workspace, working in collaboration with industry experts to strengthen cybersecurity and protect the repository of CANDU IP and information.

To help you and the work of your organizations stay safe and secure, COG's IT team has gathered cybersecurity tips and helpful hints for maintaining privacy and records as you work from home.

Use a WIFI Protected Setup (WPS) with strong encryption through your router

- Ensure you secure your home WIFI network;
  - Protect your network with a strong password;
  - Update your router's firmware settings; and
  - Don't use a public WIFI network for work activity
- Protect your personal devices;
  - Keep your computer and smartphone operating systems up-to-date;
  - Use a firewall as well as antivirus and anti-malware software;
  - Ensure these devices are password-protected; and
  - Limit users of these devices.

Be cybersecurity aware

- Email-based scams, often claiming to be urgent, from disguised email accounts, targeting remote workers;
  - Malware including ransomware can disrupt or damage devices, personal or organizational networks. Ransomware is a malicious program that blocks access to a device or account until a ransom fee is paid.
  - Malware can come from suspicious email attachments, website or hyperlink redirects, links from social media sites, false advertisements (also known as "malvertisements"), unknown USB keys, suspicious software downloads and other sources; and
- Endpoint attacks: Attacks which target home networks, devices and cloud services where company information may be more easily accessible.

Take preventive action

- Do not open unknown or suspicious emails and hyperlinks;
  - Always double-check the source email address to ensure it is not disguised;
- Avoid sharing or entering login credentials on unfamiliar systems or pages;
- Verify cybersecurity issues that claim to have a "sense of urgency";
- Activate your web browser's pop-up blocker;
- Use strong password protection on all devices;
  - Don't use the same username & password for different services; and
- Back up your files.

Alert your organization's IT services team if you encounter suspicious emails or software.

Chances are, others in your organization could be experiencing a similar issue. The safety and security of your devices and your organization's work may depend on it.