Cybersecurity Tips During COVID-19

If you have security questions, email: securityalerts@nlchi.nl.ca

Tip 1 - Use Trusted Sources of Information

- Use trusted sources of information, including government websites for up-to-date, fact-based information about COVID-19.

Tip 2 - Avoid Clicking Links

- Avoid clicking links in unsolicited emails, especially if they seem to point to legitimate COVID-19 websites. Instead of clinking the email link, go to the website directly to avoid a “masquerading site” that appears authentic, but has malicious purpose.

Tip 3 - Stay Cautious

- Stay cautious of COVID-19 email attachments, no matter the name, subject or file type.

Tip 4 - Never Reveal Personal, Financial or Patient Data

- Never reveal personal, financial or patient data or other types of sensitive information in email and do not respond to emails you suspect to be SPAM or Phishing.

Watch for typical warning signs:

- Urgent requests for information or money.
- Bad grammar and/or misspelled words.
- Unusual requests or from unusual sources.

Eastern Health | Central Health | Western Health | Labrador-Grenfell Health | Newfoundland & Labrador Centre for Health Information

Cybersecurity Tips During COVID-19

If you have security questions, email: securityalerts@nlchi.nl.ca

CONFIDENTIALITY OF HEALTH INFORMATION

During COVID-19, it is important to protect the patient data and information you have access to. Everyone is accountable for using patient data and information in an appropriate manner.

- Patient information must only be accessed to support work requirements. In health care, that is primarily by members of a patient's health care team for the purpose of providing or assisting in patient care. All access must be authorized under applicable legislation, policies and standards of practice of the Regional Health Authorities or NLCHI.
- Access to health records is audited on a regular basis to ensure that users are only accessing patient information for the purposes outlined above or for which they have authorization to access. During and following COVID-19, audits may occur more frequently.
- All staff must report real and suspected privacy and security breaches to their respective service desks. Service desks will appropriately assign to the privacy department or NLCHI security team.

HEALTH CARE THREATS

As a result of COVID-19, cyber attackers have increased their focus on health care in an attempt to access valuable information such as:

- Credentials, personal information and intellectual property;
- Sensitive data related to government response to COVID-19, or other COVID-19 topics including names of affected patients.

Health care and eHealth are current targets, including me and you:

· Healthcare workers
· Medical research
· Manufacturing
· Distribution
· Policy makers

ATTACK TYPES

1. Phishing/Malware

The majority of cyberattacks are initiated through phishing or malware emails which appear to be from a legitimate organization and related to COVID-19. These emails include malware attachments or malicious links. Examples of content from actual malicious COVID-19 emails:

Common attachment types:
.doc
.xlsx
.zip

Message Subjects:
- LATEST CORONA VIRUS UPDATES
- UNICEF COVID-19 TIPS APP
- WARNING! CORONA VIRUS

Message File Attachments:
- AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf.exe
- Coronavirus COVID-19 upadte.xlsx
- covid19.ZIP

*Lists are not exhaustive and new variants on these themes are quickly emerging.

Eastern Health · Central Health · Western Health · Labrador-Grenfell Health · Newfoundland & Labrador Centre for Health Information

Cybersecurity Tips During COVID-19

If you have security questions, email: securityalerts@nlchi.nl.ca

2. Fake Phone Applications

Many people are turning to their smartphones to seek out information about COVID-19, how it is impacting them and how they can stay safe. There have already been multiple reports of malicious applications (apps) that claim to offer information about the virus. These allow the attacker to spy on users or encrypt devices.

3. COVID-19 Websites

In the past few weeks, over 100,000 domains (URLs) have been registered containing terms like "covid," "virus" and "corona." Not all of these will be malicious, but all of them should be treated as suspect. Whether they claim to have information, a testing kit or a cure, the fact that the website didn't exist before the pandemic should make you skeptical of the URL's validity. Also, be extra, extra cautious if information is requested and **NEVER** provide sensitive data such as birth date, credit card information, MCP number or social insurance number.

RANSOMWARE

Ransomware continues to be one of the most severe threats facing health care organizations. Cyber criminals may take advantage of the pandemic and the increased pressure being placed on Canadian health organizations to extract ransom payments. The impact of a ransomware incident on Canadian organizations involved in COVID-19 response could be more severe during the current pandemic than in a non-crisis environment.

Eastern Health | Central Health | Western Health | Labrador-Grenfell Health | Newfoundland & Labrador Centre for Health Information