NUCLEUSLABS

phone 604.585.7250 *facsimile* 604.648.8916 *toll free* 1.888.266.8888
C200-9801 King George Boulevard, Surrey, British Columbia V3T 5H5

Best Practice Tips for Data Security and Privacy

As one of Community Living Ontario's Strategic Technology Partners, we'd like to offer some simple advice around security and privacy of data, that some agencies may find helpful.

Over the past month, we have recognized that many agencies have adapted their programs and services due to the COVID-19 pandemic. As a result, we have seen agencies allow access to secure systems and data for staff working at home, or other off-site locations. In some cases, front-line, management and administrative staff are using personal devices and/or computers to conduct business. Or they may have taken agency-supplied devices home to enable them to keep providing service.

In light of these unique circumstances, here are some quick reminders of basic security and privacy practices that all staff should be doing:

1. If you are using a personal (or agency-supplied) device/computer to communicate with staff and conduct business from home:

   a) Ensure that your operating system and web browser are fully up-to-date.
      - How to update Windows Computers https://support.microsoft.com/en-ca/help/12373.
      - How to update Apple OSX Computers https://support.apple.com/en-ca/guide/mac-help/mchlpx1065/mac.
      - How to update Apple iOS Devices https://support.apple.com/en-ca/HT204204.

   b) Ensure that your device/computer has both anti-virus and anti-malware software installed and that they are up-to-date.

   c) Ensure that all passwords used for accessing your agency's services (email, file servers, etc.) follow the best practice guidelines:
      - At least 8 characters, mixture of upper- & lower-case letters
      - A mixture of letters & numbers or special characters.

      Note: Some agencies use more stringent guidelines, so please follow your agency's policy.

   d) Make sure to change your passwords as per best practice guidelines - every 21 days or sooner. Some agencies have a more frequent password reset period, so please follow your agency's policy.

2. Sharing of person-served information such as documents, notes and messages should not be done through email, text message or social media messaging, as these methods are quite insecure. This includes the sharing of word documents, excel documents, PDF files, etc.
   Additionally, use of Dropbox, Box, Google Docs or other publicly-available file sharing services are not regarded as secure. These services are typically housed outside of Canada and the information stored on these services is not held as private by the corporations providing them.

   Note: For NucleusLabs' partner agencies, sending of files and messages can be done safely through our secure Com-Box messaging system as usual.

phone 604.585.7250 *facsimile* 604.648.8916 *toll free* 1.888.266.8888
C200-9801 King George Boulevard, Surrey, British Columbia V3T 5H5

3. If you are accessing your agency's secure servers from remote locations, you should be using some form of VPN (Virtual Private Network) technology. A VPN creates a secure connection to another network over the Internet, encrypting the data transmitted between sites.

If you have any questions or concerns about your agency's use of technology during the COVID-19 pandemic, feel free to contact NucleusLabs at 1-888-266-8888 ext. 2 or reach out to us at info@nucleuslabs.com.

The NucleusLabs' team recognizes the uniqueness of the current realities and we want to ensure you and your staff are supported in every way so that the people you serve can continue to access the best care possible.

Warmly,

Crystal Wuthrich and the NucleusLabs Team