



## IT & Cybersecurity during COVID-19 / Coronavirus

The pandemic is prime time for cyber criminals to wreak havoc. Almost as quickly as the virus grew in our country, hackers were launching phishing attacks, trying to capitalize on the increased demand for information and guidance. Cybersecurity has never been as imperative as it is today. Non-profit housing providers and their tenants must not only rely on their ability to prevent attacks, but also to detect and respond to them. It is more critical than ever to have well-established security measures in place that guides investment of finite resources and helps ensure risk is mitigated to an acceptable level.

Basic security measures to keep in mind:

- Verify email/social media links/files with the sender before clicking on them
- Stay patched and up to date
- Make sure your backups are working
- Secure your accounts with strong passphrases and use multi-factor authentication where possible

Specific resources for your members:

Working From Home Securely

[This guide sheet](#) covers the basics of security for an “at home” worker.

COVID-19 related Phishing & Social Engineering Videos / Info

- [RCMP: Fraud and Cyber Crime Prevention Message](#) (3 min)
- [How to Avoid COVID-19 Cybersecurity Scams](#) (30 min)
- [Canadian Centre for Cyber Security: Cyber Hygiene for COVID-19](#)

E-Learning

- [Terranova Security COVID-19 Kit](#)
- [Terranova Security Work from Home Kit](#)

This Canadian e-learning company provides some online modules to educate users on how to avoid COVID-19 scams, as well as tips on working from home.

*\* It does ask for an email address and your consent to market to you.*

Interactive Quiz: Can I Be Phished? – Covid-19 Edition

- [Can I Be Phished? – COVID-19 Edition](#)

This Canadian e-learning company provides an interactive “phishing test”.

*\* It does ask for an email address and your consent to market to you, but the experience is valuable worth the time.*