

CYBER SECURITY ADVICE AND GUIDANCE FOR RESEARCH AND DEVELOPMENT ORGANIZATIONS DURING COVID-19



To help address the novel coronavirus (COVID-19) pandemic, governments in Canada are investing millions of dollars into research and development related to combatting current and future outbreaks of COVID-19 and other similar threats.

Cyber threat actors know that there is a lot of pressure on governments, the healthcare sector, and Canadian businesses and academic institutions to help slow the spread of COVID-19, and they are taking advantage of this pandemic to carry out malicious and fraudulent activities. In this case, cyber threat actors are targeting businesses and institutions involved in research and development, and they may even pose as a legitimate business to try to spread misinformation, obtain sensitive information, or gain funding.

To help you during this time, we curated a selection of our advice and guidance products. **Don't wait until there's an incident to get to know us. If you have questions, want to find a complete list of our guidance products, or sign up for our services, come visit us at the Cyber Centre website: cyber.gc.ca/**



CYBER SECURITY BEST PRACTICES

- [Cyber Hygiene for COVID-19](#)
- [Protecting High-Value Information: Tips for Small and Medium Organizations \(ITSAP.40.001\)](#)
- [Cyber Security Tips for Remote Work \(ITSAP.10.116\)](#)
- [Benefits and Risks of Adopting Cloud-Based Services in Your Organization \(ITSE.50.060\)](#)
- [Best Practices for Passphrases and Passwords \(ITSAP.30.032\)](#)
- [Spotting Malicious Email Messages \(ITSAP.00.100\)](#)
- [Don't Take the Bait: Recognize and Avoid Phishing Attacks](#)
- [Protect Your Organization From Malware \(ITSAP.00.057\)](#)
- [Ransomware: How to Prevent and Recover \(ITSAP.00.099\)](#)
- [Internet of Things Security for Small and Medium Organizations \(ITSAP.00.012\)](#)
- [Using Bluetooth Technology \(ITSAP.00.011\)](#)
- [How Updates Secure Your Device \(ITSAP.10.096\)](#)

BASELINE CYBER SECURITY CONTROLS

The [Baseline Cyber Security Controls for Small and Medium Organizations](#) lists a set of lower-cost and lower-burden security controls that you can implement to thwart cyber threat actors, reduce exposure to cyber threats, and get the most out of your cyber security investments. These controls are organized into thirteen groups:

- Have an incident response plan
- Patch operating systems and applications automatically
- Enable security software
- Configure devices securely
- Use strong user authentication
- Provide employee training
- Back up and encrypt data
- Secure mobility
- Establish perimeter defences
- Secure cloud and outsourced IT services
- Secure websites
- Have access control and authorization
- Secure portable media

To help you get started with these controls, you can read through our related guidance (linked on the left) on cyber security best practices.

[CyberSecure Canada](#) is Canada's national certification program. This program certifies small and medium organizations that implement the baseline controls.

ADDITIONAL INFORMATION

- [Cyber Security for Small and Medium Organizations](#)
- [CyberSafe: Protect Your Business](#)
- [Canadian Shield—Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic](#)
- [Alerts and Advisories](#)
- [RSS feed](#)

Your organization may not have the resources or capacity for in-house security services. If you want to work with a managed service provider, see our information bulletin:

[Contracting with Managed Service Providers](#)

