

## **Caution: Cyber Security Campaign Targeting COVID-19 Researchers**

The Canadian Center for Cyber Security (CCCS) has advised of an active and sophisticated cyber security campaign targeting COVID-19 researchers. The campaign leverages a phishing email to spread ransomware that could disrupt research activity.

The CCCS is advising that all researchers, and in particular those working on COVID-19 related research, exercise elevated levels of caution with email attachments and links. More information about the attack is available at the [CCCS website](#).

The University of Guelph Information Security team is watching this situation closely and has dedicated security analysts monitoring our networks for these threats.

You can find additional cyber security resources on our website (<https://infosec.uoguelph.ca>) including more details on COVID-19 security threats and guidance on working remotely. All of these documents are being updated regularly as new information becomes available:

- [COVID 19: Stay Calm and Don't Get Scammed](#)
- [Working from Home Securely](#)
- [Working Remotely](#)

Please reach out to the Information Security team ([infosec@uoguelph.ca](mailto:infosec@uoguelph.ca)) or the CCS Help Centre ([ITHelp@uoguelph.ca](mailto:ITHelp@uoguelph.ca)) if you have any questions or concerns.

Alert ClassificationsCategory:

Research Management and Support

### **Disciplines:**

Health and Life Sciences

Humanities

Information and Communications Technology

Physical Sciences and Engineering

Social Sciences

---

### **Source**

**URL:** <https://www.uoguelph.ca/research/alerts/content/caution-cyber-security-campaign-targeting-covid-19-researchers>