Research Security Information Update

May 2021

AT A GLANCE:

The Research Security Information Update is an unclassified open-source collation, produced by Public Safety Canada's Safeguarding Science team, on issues considered relevant to Canada's broad research security interests. Its purpose is to provide specialized research security-focused information to the Canadian research community. Each update could include a round-up of recent and relevant developments, information on a specific research security related topic, relevant case study briefs, cyber security related statistics, trends and tips.

What is Research Security?

Broadly speaking, research security refers to the measures that protect knowledge, technologies, and data that could assist in the advancement of a foreign threat actor's geopolitical, economic, and security interests to the detriment of Canada's. The target assets can vary from applications in weapons of mass destruction programs (i.e., chemical, biological, radiological, and nuclear) to dual-use technologies (i.e., technologies with both civilian and military applications), such as artificial intelligence, quantum computing, and bio- and nanotechnology, to intellectual property and confidential information used for research.

Notable Developments in Research Security

April 2020 – In the context of COVID-19 vaccine development, the Canadian Security Intelligence Service (CSIS) began delivering threat briefings to the biopharmaceutical sector, including Canadian universities.

May 14, 2020 – CSE and CSIS released a joint statement warning the Canadian research community that data and technologies linked to pandemic research have become attractive targets for state-sponsored actors.

September 14, 2020 – The Ministers of Innovation, Science and Economic Development, Public Safety, and Health released a statement encouraging all members of the Canadian research community to take extra precautions to safeguard all research, technology and development relating to COVID-19 vaccines and therapeutics.

September 14, 2020 – The Canadian Government launched the Safeguarding Your Research Portal – developed by a joint Government of Canada-Universities Working Group – to provide the research community with guidance, information, and tools to help them protect their research and intellectual property.

September 17, 2020 – The Canadian Centre for Cyber Security released a publication on "Security Considerations for Research and Development". Research organizations are encouraged to review the publication to gain information on how to protect their research environment and data, how their organization should understand common cyber security threats and how to implement some basic security measures.

November 16, 2020 – The Canadian Centre for Cyber Security published the National Cyber Threat Assessment for 2020.

January 15, 2021 – The Government of Canada mandated the Minister of Public Safety to work closely with the Canadian research community and the Minister of Innovation, Science and Industry to continue to safeguard Canada's world-leading research.

ISBN: PS9-20/2021E-PDF 978-0-660-37941-8

February 9, 2021 – Remarks by the Director of CSIS to the Centre for International Governance Innovation outlined how Canadian companies in almost all sectors of the economy have been targeted by hostile foreign actors. He noted that "today our adversaries are more focused on intellectual property and advanced research held on computer systems in small start-ups, corporate boardrooms, or university labs across the country."

March 24 , 2021 - The Minister of Innovation, Science and Industry, Minister of Public Safety Canada and Minister of Health released a statement committing to support a research environment that is open and collaborative while also safeguarding the integrity of Canada's research enterprise, national security, and long-term economic competitiveness and prosperity.

Current Research Security Efforts

The intent of all research security efforts is to ensure that hard-earned Canadian research is not misused or exploited, and that the Canadian research community gets the maximum benefit of their work. These issues are explained in the *Building Security Awareness in the Academic Community* document that Public Safety Canada published in 2019. Below is a brief overview of some of the current research security considerations and efforts (various initiatives, policies, programs, etc.) that are being implemented in Canada and by a number of our partners.

Australia

In November 2019, Australia published *Guidelines to counter foreign interference in the Australian university sector* ('the guidelines'). The guidelines were developed for, and in partnership with, the university sector to deepen resilience against foreign interference risks. They build on risk management policies and security practices already implemented by Australian universities and assist decision-makers to assess the risks from foreign interference, while supporting an environment of trust, so Australian universities can continue to produce world-class research.

Canada

Canada has been raising awareness of research security issues through Safeguarding Science since 2016. Safeguarding Science is being expanded to provide additional resources to Canadian academic, research and development sectors, as well as programs to enhance institutional capacity to address research security issues. Moreover, in September 2020, Canada launched the Safeguarding Your Research portal to disseminate guidance and tools for researchers and research administrators.

New Zealand

The Government of New Zealand has been working with Universities New Zealand to raise awareness of research integrity and security issues and to develop joint guidance for the academic community. This collaboration will build upon the existing policies for research integrity and ethics maintained by the New Zealand Royal Society and individual universities.

United States

Since mid-2018, the US has introduced a range of new and revised rules, policies and regulations to address concerns about foreign interference in research and the theft of intellectual capital. Various departments and agencies have introduced new measures to address risks to the integrity of the research enterprise, such as the establishment of the Joint Committee on Research Environment by the Office of Science and Technology Policy at the White House.

United Kingdom

In 2019, the UK's Centre for the Protection of National Infrastructure published its "*Trusted Research Guidance*", which provides recommendations on how the UK's research community can protect their personal and research-related data from foreign interference and theft.

Cyber Security Insight

Canadian research institutions heavily rely on the cyber infrastructure, whether at the institutional or national level, to conduct research, store data, and run experiments. This reliance, especially during the COVID-19 pandemic, has increased the vulnerability of Canadian institutions, that are at a higher risk of losing valuable research through cyber-attacks or attempts by threat actors to infiltrate Canadian cyber infrastructure. You can help yourself and your institution by considering the following tips:

ISBN: PS9-20/2021E-PDF 978-0-660-37941-8

Common Attack Techniques: Cyber threat actors can use different methods to tamper with or steal your research data and intellectual property. *Phishing (Figure 1)* can leave your systems vulnerable to threat actors deploying ransomware on your devices/networks. To prevent a phishing attack, look out for elements of malicious communication *(Figure 2*).

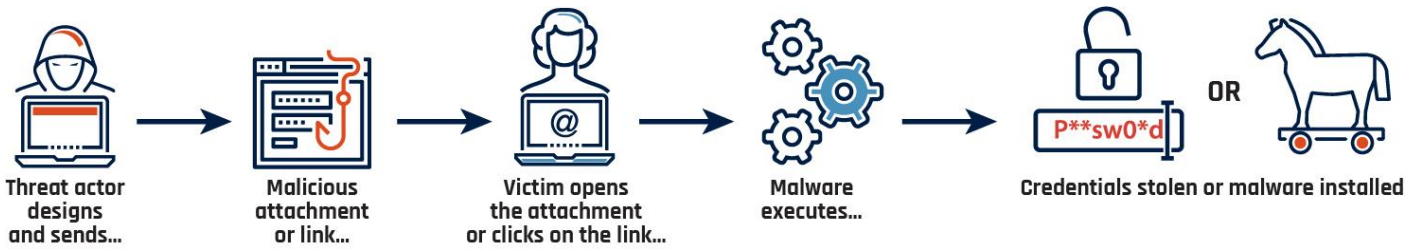


Figure 1: Phishing and Spear-Phishing (Reference: Annex A: The Cyber Threat Toolbox)

Figure 2: The Elements of Malicious Communication (Reference: NCTA 2020)

Ransomware *(Figure 3*) is a type of malware that will make your data inaccessible (e.g., locking systems and encrypting all files) until a ransom is paid. *For more information, see ITSAP.00.099 Ransomware: How to Prevent and Recover.*

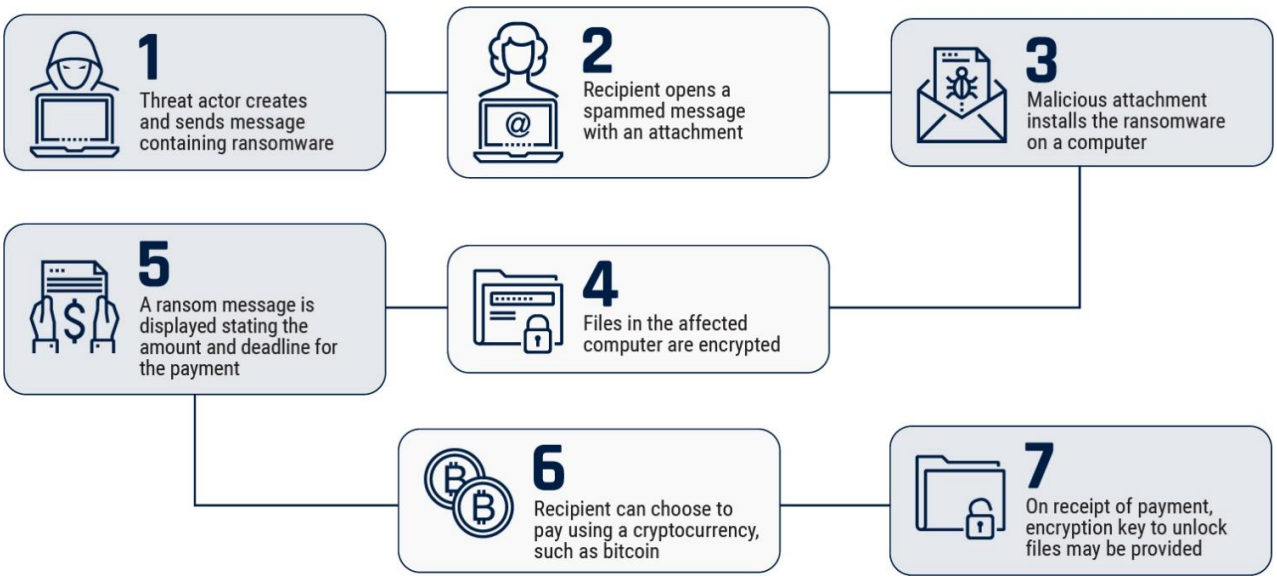


Figure 3: Ransomware (Reference: Annex A: The Cyber Threat Toolbox)

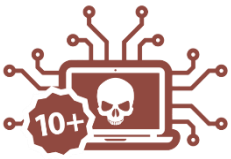
ISBN: PS9-20/2021E-PDF 978-0-660-37941-8

Don't Be the Weak Link! - *"The remote workforce is being increasingly targeted by state-sponsored threat actors and cybercriminals. Cyber threat actors are attempting to identify individuals working at home employed in areas of strategic interest and are exploiting technologies deployed in support of a remote workforce, such as virtual private networks (VPNs) or video-conferencing platforms."*

(Reference: NCTA 2020)

5 Tips to Improve your Cyber Security at Home:

1. Use a complex/strong unique password. Do not share.
2. Apply updates to your devices regularly.
3. Install antivirus security tools.
4. Be vigilant of phishing emails.
5. Use an off-line method to back up your data.



21%
Percentage of Canadian organizations surveyed that faced more than 10 attacks in 2019.

(Reference: 2020 CIRA Cybersecurity Report)


80%
Percentage of Canadian organizations surveyed that faced a cyber-attack in 2019.

(Reference: 2020 CIRA Cybersecurity Report)

Want to know more?

Need help or have questions? Want to stay up to date and find out more on all things research security? Please send us an email at safeguardingscience-scienceensecurite@ps-sp.gc.ca or visit our Safeguarding Science webpage.

Public Safety Canada aims to continually publish useful information to the Canadian research community on relevant research security issues. We would like to hear from you! Are there specific products, tools, or information you would like to receive (i.e. on emerging risks/threats, research security case studies, statistics, guidance on key issues, security best practices, etc.)? Please send any suggestions you have to the Safeguarding Science email listed above.

Want to Report an Incident?

RCMP – National Security Information Network (NSIN)
Reporting of unrecognized persons, suspicious incidents, or computer-related activities.

Phone: 1-800-420-5805 Email: NSIN_RISN@rcmp-grc.gc.ca

Canadian Security Intelligence Service (CSIS)
Reporting of potential non-urgent national security threats or suspicious activities.

Phone: 1-800-267-7685 Website: Reporting National Security Information

Canadian Centre for Cyber Security (CCCS)
The CCCS Contact Centre is the single point of contact for questions on Cyber Security.

Phone : 1-833-CYBER-88 Email: contact@cyber.gc.ca

Please note that there is no planned publication schedule for the Research Security Information Update. Public Safety Canada will provide information as it arises or becomes available to our audience.

ISBN: PS9-20/2021E-PDF 978-0-660-37941-8