For Immediate Release

# Click this Link! Or Should I?

**May 28, 2020** – For the truly nefarious, even a crisis is an opportunity. Canadian, American and European authorities have noticed an uptick in cybercrime incidents as more people work from home. Together, corporate and government employees could be facing billions of dollars in additional costs from ransomware, phishing or malware attacks.

Everyone knows the classic email from a Prince from another country needing all kinds of money to get away. But cybercriminals are getting smarter. In fact, the briefing note states that as authorities and resources are focused on fighting the COVID-19 pandemic, now is the perfect time to target vulnerable internet users who may be working from home for the first time.

From phishing emails to misinformation, organizations from all around the world have seen a spike in cybercrime and scams. "To protect citizens and states, tools such as end-to-end encryption and zero-trust architecture need to be deployed in mainstream applications" said author David Bruno, who is the founder and CEO of SafeSwiss, a global cyber security firm.

Standard solutions recommended by experts:

**End-to-end encryption (E2EE):** This method facilitates the type of encrypted communication that only the sender and receiver can read or see.

**Zero-Trust Architecture (0-trust):** This method goes further than simply encrypting the file, it stores it on a virtual server that is placed behind a firewall.

Combining these two cutting-edge techniques could deliver a platform government institutions, medical researchers and individuals need to safeguard their sensitive research information/data.

This white paper is a piece that was originally published by David Bruno in March 2020.

To read *COVID-19 and CyberCrime: How rogue nations and cyber criminals are exploiting a global crisis,* follow the link: https://www.northernpolicy.ca/covid-19-and-cybercrime

-30-

**Media Interviews:** Author David Bruno (English and Français) and NPI Research Manager Rachel Rizzuto are available for comment. To arrange an interview, please contact:

Christine St-Pierre
Communications Coordinator
226-344-3213
cstpierre@northernpolicy.ca

***About Northern Policy Institute:***

*Northern Policy Institute is Northern Ontario's independent think tank. We perform research, collect and disseminate evidence, and identify policy opportunities to support the growth of sustainable Northern communities. Our operations are located in Thunder Bay and Sudbury. We seek to enhance Northern Ontario's capacity to take the lead position on socio-economic policy that impacts Northern Ontario, Ontario, and Canada as a whole.*

***About the author:***

*David Bruno*

*As founder and CEO of a global cyber security firm, David Bruno specialises in anti-fraud and anti-corporate espionage systems for banks and financial institutions worldwide. Through his company, Secure Swiss Data (now SafeSwiss®), he provides financial sector solutions for the digital and interactive e-commerce sectors. For 20 years he has worked to provide security protection to the masses. After completing his MA in International Relations & Communications in Spain, he was hired by a telecom company for their new office, working out of both Barcelona and Montreal as a business development manager. It was here that his career advocating for fraud prevention systems began. He has since taken a number of courses in topics including DDoS, identity theft, anti-money laundering and combating terrorist financing.*

*On the fraud prevention count, David has a number of initiatives on the go. He has found a stigma attached to anyone who seeks privacy, in that they can sometimes be viewed as having something to hide. To further the interests of personal protection in the cyber world, he is working to change this perception so more will feel emboldened to act. He has invested his own money in a free encrypted email server for the public. Born of immigrant parents, he understands the challenges they face and makes a considerable effort to help refugees through the web site or at conferences. He educates on the surveillance of email in general and the importance of encryption, especially for vulnerable populations. He teaches ethics and anti-money laundering courses in the Canadian Region, and is working with the government on the development and refinement of its new digital charter, a cyber security policy named "Canada's Digital Charter".*