NORTHERN POLICY INSTITUTE | INSTITUT DES POLITIQUES DU NORD

Note d'information No. 17 | Mai 2020

COVID-19 et la cybercriminalité : États voyous et cybercriminels – exploiteurs de crise mondiale

Par : David Bruno

Qui nous sommes

Conseil d'administration : Le conseil d'administration détermine l'orientation stratégique de l'Institut des politiques du Nord. Les administrateurs font partie de comités qui s'occupant de finance, de collecte de fonds et de gouvernance; collectivement, le conseil demande au chef de la direction de rendre des comptes au regard des objectifs de nos objectifs du plan stratégique. La responsabilité principale du conseil est de protéger et de promouvoir les intérêts, la réputation et l'envergure de l'Institut des politiques du Nord.

Président et Chef de la direction : recommande des orientations stratégiques, élabore des plans et processus, assure et répartit les ressources aux fins déterminées.

Conseil consultatif : groupe de personnes engagées et qui s'intéressent à aider l'institut des politiques du Nord mais non à le diriger. Chefs de files dans leurs domaines, ils guident l'orientation stratégique et y apportent une contribution; ils font de même en communication ainsi que pour les chercheurs ou personnes-ressources de la collectivité élargie. Ils sont pour de l'institut des politiques du Nord une « source de plus mûre réflexion » sur l'orientation et les tactiques organisationnelles globales.

Conseil consultatif pour la recherche : groupe de chercheurs universitaires qui guide et apporte une contribution en matière d'orientations potentielles de la recherche, de rédacteurs possibles, d'ébauches d'études et de commentaires. C'est le « lien officiel » avec le monde universitaire.

Évaluateurs-homologues : personnes qui veillent à ce que les articles spécifiques soient factuels, pertinents et publiables.

Rédacteurs et associés : personnes qui offrent, au besoin, une expertise indépendante dans des domaines spécifiques de la politique.

Outils d'engagement permanent (grand public, intervenants du gouvernement, intervenants de la collectivité) : Veiller à ce que l'Institut des politiques du Nord reste à l'écoute de la communauté.

Ce rapport a été rendu possible grâce au soutien de notre partenaire, la Société de gestion du Fonds du patrimoine du Nord de l'Ontario. L'Institut des politiques du Nord exprime sa grande appréciation pour leur généreux soutien, mais insiste sur ce qui suit : Les points de vue de ces commentaires sont ceux de l'auteur et ne reflètent pas nécessairement ceux de l'Institut, de son conseil d'administration ou de ceux qui le soutiennent. Des citations de ce texte, avec indication adéquate de la source, sont autorisées.

Les calculs de l'auteur sont basés sur les données disponibles au temps de publication et sont sujets aux changements. T

raduit par: Renée Allard O'Neil

Published by Northern Policy Institute
874 Tungsten St.
Thunder Bay, Ontario P7B 6T6
ISBN: 978-1-989343-85-2

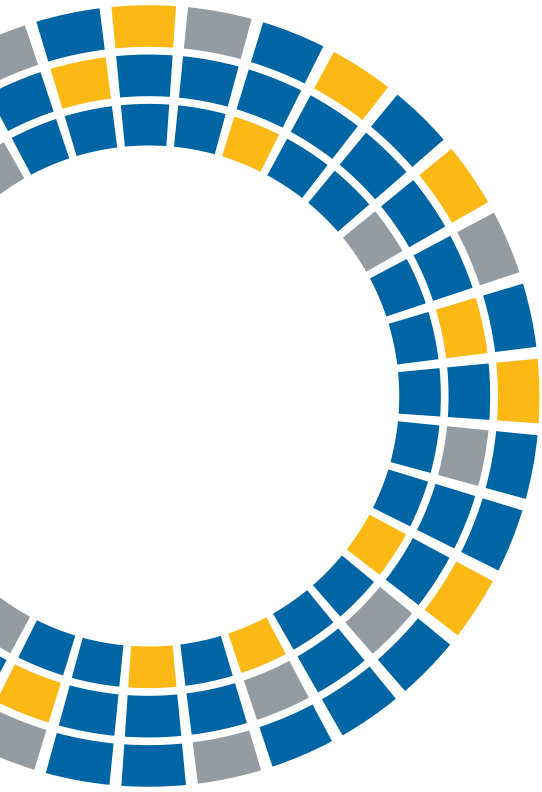
À propos de l'auteur

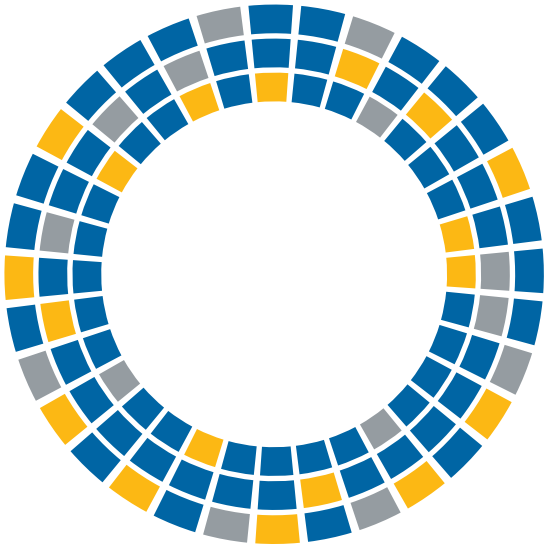
David Bruno

En tant que fondateur et PDG d'une entreprise mondiale de cybersécurité, David Bruno est spécialisé dans les systèmes anti-fraude et anti-espionnage d'entreprise pour les banques et les institutions financières du monde entier. Par le biais de son entreprise, Secure Swiss Data (désormais SafeSwiss®), il fournit des solutions du secteur financier pour les secteurs du commerce électronique numérique et interactif. Pendant 20 ans, il a travaillé pour fournir des protections de sécurité aux masses. Après avoir terminé sa maîtrise en relations internationales et communications en Espagne, il a été embauché par une entreprise de télécommunications pour leur nouveau bureau, travaillant à Barcelone et à Montréal en tant que directeur du développement commercial. C'est ici que sa carrière de défenseur des systèmes de prévention de la fraude a commencé. Il a depuis suivi un certain nombre de cours sur des sujets tels que les DDoS, le vol d'identité, la lutte contre le blanchiment d'argent et la lutte contre le financement du terrorisme.

Sur le plan de la prévention de la fraude, David a un certain nombre d'initiatives en cours. Il a trouvé une stigmatisation attachée à toute personne qui recherche la vie privée, en ce sens qu'elle peut parfois être considérée comme ayant quelque chose à cacher. Pour promouvoir les intérêts de la protection personnelle dans le cyber-monde, il travaille à changer cette perception afin que plus se sentent encouragés à agir. Il a investi son propre argent dans un serveur de messagerie crypté gratuit pour le public. Né de parents immigrants, il comprend les défis auxquels ils sont confrontés et déploie des efforts considérables pour aider les réfugiés via le site Web ou lors de conférences. Il éduque sur la surveillance du courrier électronique en général et sur l'importance du chiffrement, en particulier pour les populations vulnérables. Il donne des cours d'éthique et de lutte contre le blanchiment d'argent dans la région du Canada et travaille avec le gouvernement à l'élaboration et au perfectionnement de sa nouvelle charte numérique, une politique de cybersécurité appelée «Charte numérique du Canada».

Table des matières





Résumé

La crise actuelle présente une occasion en or pour ceux et celles aux intentions infâmes. Avec un nombre croissant de personnes en télétravail, les autorités canadiennes, américaines et européennes ont observé un rebond de cybercriminalité. Une menace qui continue de s'élargir alors que plusieurs employés du gouvernement et du corps législatif travailleront à distance cette semaine. Ensemble, les secteurs privé et gouvernemental pourraient être confrontés à des milliards de dollars en dépenses supplémentaires pour prévenir les attaques par rançongiciels, d'hameçonnage ou de logiciels malveillants. Au cours des dernières années, les informations qui circulent sur les réseaux informatiques sont devenues un enjeu majeur de sécurité. Parmi les attaques, les plus audacieuses sont celles des autorités gouvernementales de la Russie, de l'Iran et de la Corée du Sud. Dans le but de protéger l'État, ses citoyennes et citoyens, des outils tels que le chiffrement de bout en bout et des modèles à vérification systématique («Zero Trust») doivent être déployés dans les applications courantes.

Bien que ce document vise principalement à garantir un périmètre de réseau solide, il faut également reconnaître que les utilisateurs doivent être éduqués, car ils sont sans doute la partie la plus faible de tout réseau.

Ce livre blanc a été publié à l'origine par David Bruno en mars 2020. Il peut être consulté en cliquant sur le lien suivant : https://davidbruno.ca/

Introduction

La crise actuelle présente une occasion en or pour ceux et celles aux intentions infâmes. Selon Paddon (2020), les autorités canadiennes et américaines ont constaté une hausse de cybercriminalité en parallèle au nombre d'individus en situation de télétravail. De son côté, Sharton (2020) estime que les cybercriminels profitent du fait que les autorités et les ressources sont concentrées sur la lutte contre la pandémie actuelle et ciblent les internautes vulnérables pour qui il s'agit d'une première expérience de télétravail. «Éventuellement, les entreprises pourraient être confrontées à la perspective d'une exploitation avec peu, sinon aucun, personnel sur place ou avec des équipes de TI réduites et autres services d'assistance importants», souligne Sharton.

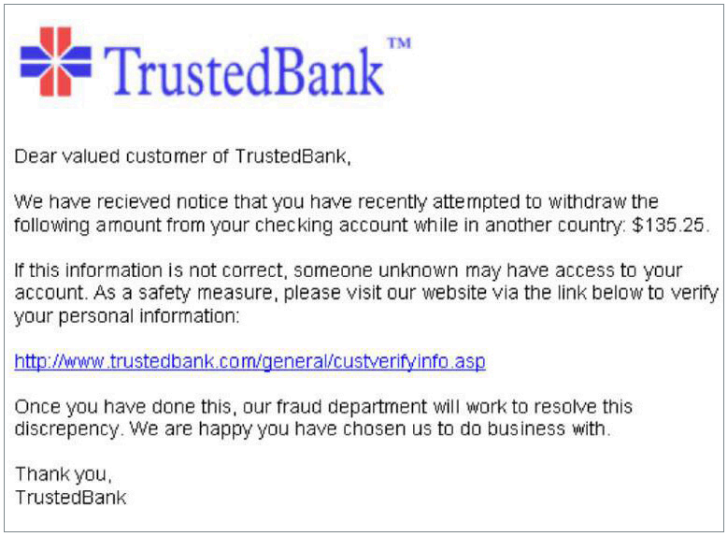
Par ailleurs, 85 % des dirigeants d'entreprises interrogés par le CNBC Technology Executive Council ont répondu qu'au moins la moitié de leurs employés travaillaient à partir de la maison alors que 36 % d'entre eux constataient une hausse de menaces à la sécurité d'information (Rosenbaum, 2020). Un dirigeant a également noté que le nombre d'incidents d'hameçonnage et de fraudes en ligne avait augmenté de 40 % depuis le début de la pandémie. Outre-Atlantique, les entreprises britanniques ont signalé une hausse de 400 % des menaces à la cybersécurité au cours des six dernières semaines (Corfield, 2020).

Selon les experts de cybersécurité, les menaces les plus courantes sont l'hameçonnage et les attaques de rançongiciels et de logiciels malveillants. C'est qu'en effet plusieurs employés sont peu habitués à se connecter au réseau privé virtuel («RPV») de leur employeur. Compte tenu la propagation rapide de la COVID-19, il semble probable que les entreprises aient précipité les instructions fournies aux employés afin qu'ils puissent effectuer leur travail à distance créant ainsi de graves vulnérabilités exploitables par les cybercriminels. Même dans les cas où la connexion RPV est sécurisée, les pirates informatiques repèrent et profitent des vulnérabilités des réseaux et connexions Internet privés (Doffman, 2019).

Cette menace continue de s'élargir alors que plusieurs employés du gouvernement et du corps législatif travailleront à distance cette semaine. Depuis avoir adopté le télétravail, Nicole Coughlin Raimundo, dirigeante principale de l'information pour la ville de Cary dans l'état de la Caroline du Nord, remarque une augmentation du nombre d'attaques d'hameçonnage auxquelles son équipe est confrontée. Bien que les services des TI aient déployé des mesures de cybersécurité comme des solutions antivirus, des dispositifs d'extrémité et de l'assistance à distance, il est fort probable que les réseaux à domicile des employés ne soient pas aussi sécuritaires (Rosenbaum, 2020).

Ensemble, les secteurs privé et gouvernemental pourraient être confrontés à des milliards de dollars en dépenses supplémentaires pour prévenir les attaques par rançongiciels, d'hameçonnage ou de logiciels malveillants. Par conséquent, les coûts globaux de la cybersécurité pourraient avoir des effets dévastateurs sur l'ensemble de l'économie — au moment même où la récession frappe — et s'ajouter aux coûts auxquels sont confrontés les utilisateurs et les contribuables. Cependant, il semble y avoir une autre dimension fortement regrettable qui s'ajoute au fardeau économique, celle des cyberattaques parrainées par l'État.

Figure 1: Exemple d'hameçonnage



Andrew Levine/Domaine public
https://commons.wikimedia.org/w/index.php?curid=549747.

Une panique commanditée par l'État

Au cours des dernières années, les informations qui circulent sur les réseaux informatiques sont devenues un enjeu majeur de sécurité. D'après Bradshaw & Howard (2019), le nombre de pays qui exploitent la désinformation en ligne à des fins politiques est passé de 28 en 2017 à 70 en 2019. Parmi ceux-ci, les gouvernements les plus notables répandent également de fausses informations dans leur pays, sans compter les pays rivaux.

Durant cette crise sanitaire, les plateformes de médias sociaux en Iran, en Chine, au Venezuela et en Égypte ont été inondées d'allégations fausses et trompeuses et de théories du complot qui ont provoqué une détresse et une panique généralisées (Beavers, 2020).

La majorité de celles-ci sont axées sur les origines du virus de la COVID-19 et les intentions de ses créateurs.

Parmi les attaques les plus audacieuses sont celles des autorités gouvernementales de la Russie, de l'Iran et de la Corée du Sud. Selon une note d'informations interne de l'Union européenne, les médias russes partenaires de l'État ont lancé une importante campagne de désinformation contre l'Occident dans le but d'aggraver les répercussions du coronavirus, de générer la panique et de semer la méfiance (Emmott, 2020). «Pour le Kremlin, la Covid-19 est une opportunité autant qu'une crise», souligne Foxall (2020). «La Russie a longtemps cherché à subvertir l'ordre international fondé sur des règles en créant des fractures au sein des sociétés occidentales, ou en profitant des ruptures existantes».

Conçues comme des publications devenues virales, ces fausses déclarations comprennent des accusations selon lesquelles le virus fut importé par des migrants illégaux, que celui-ci soit une arme biologique développée par la Chine ou un outil des États-Unis destiné à affaiblir d'autres nations (Jozwiak, 2020).

Il est à noter que la campagne de désinformation du Kremlin ne vise pas seulement l'étranger. Selon les experts de la santé, l'administration du président russe Vladimir Poutine aurait également réduit le nombre de cas signalés du coronavirus pour empêcher le public de reconnaître l'ampleur de la crise (Greenberg & Fomina, 2020). Ainsi, en date du 18 mars, la Russie n'avait que signalé 147 cas de coronavirus et aucun décès malgré sa population de 140 millions d'habitants.

Figures 2: Exemple de désinformation

Source: Lim, 2020

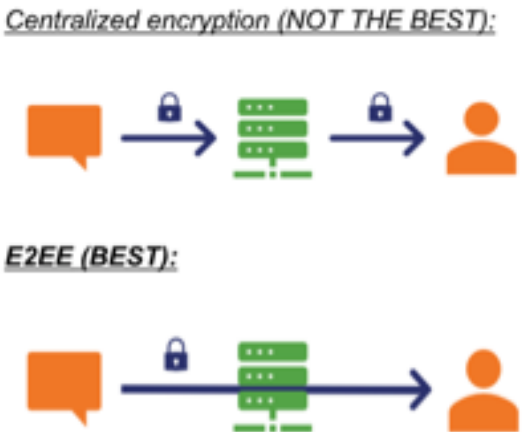
Solutions

Dans l'ensemble, les gouvernements ont durci le ton en ce qui a trait à la désinformation. Le Centre de la sécurité des télécommunications du Canada a déclaré avoir démantelé de faux sites Web se présentant comme des organismes gouvernementaux. Celui-ci a également déclaré que les organismes de la santé canadiens font face à un «niveau de risque élevé» en ce qui a trait aux incidents de cybersécurité (Tunney, 2020).

L'arsenal du gouvernement en matière de cybersécurité peut néanmoins être limité puisque celui-ci mène une guerre sur plusieurs fronts. Alors que les infrastructures gouvernementales et les données des citoyens sont vulnérables aux cyberattaques, que ce soit d'autres pays ou des malfaiteurs disposant d'outils sophistiqués, les nations ont également besoin de protection tout aussi robuste.

Pour contrer ces risques, les experts recommandent le chiffrement de bout en bout («end-to-end encryption» ou E2EE), une solution qui permet de chiffrer les données d'un message afin que seuls l'expéditeur et le destinataire puissent les voir. Il s'agit d'une mesure très efficace. Plusieurs gouvernements, dont ceux de l'Australie, du Royaume-Uni et des États-Unis, ont tenté de bloquer son utilisation par Facebook sur sa plateforme WhatsApp (Thakkar, 2019), preuve que cette démarche pourrait supplanter les capacités des agences nationales de renseignement et être un outil efficace pour protéger les données privées, sensibles ou classifiées.

Figure 3: E2EE vs Centralized Encryption



Une autre solution novatrice, le partage de fichiers de type «Zero Trust» (ou 0-trust). Développé en 2010 par l'analyste principal chez Forrester Research Inc., John Kindervag, le modèle à vérification systématique aussi nommé le Zero Trust Network ou Zero Trust Architecture, est en passe d'être adopté par le grand public (Pratt, 2018). Au-delà du cryptage de fichier, cette solution stocke également les fichiers sur un serveur virtuel protégé par un pare-feu.

Puisqu'ils n'ont jamais besoin de stocker, télécharger ou partager leurs fichiers, les employés peuvent avoir accès aux dossiers depuis n'importe quel endroit et avec n'importe quel appareil.

Ensemble, ces deux mesures de pointe pourraient fournir aux institutions gouvernementales et aux chercheurs en santé une plateforme idéale pour sauvegarder les données sensibles tout en offrant une nouvelle solution dans la lutte contre la désinformation liée à la COVID-19. C'est la raison pour laquelle SafeSwiss a fusionné le chiffrement E2EE avec le modèle à vérification systématique «Zero Trust» de FileFlex, une plateforme d'accès aux données à distance et une infrastructure informatique hybride développée par la société canadienne QNEXT.

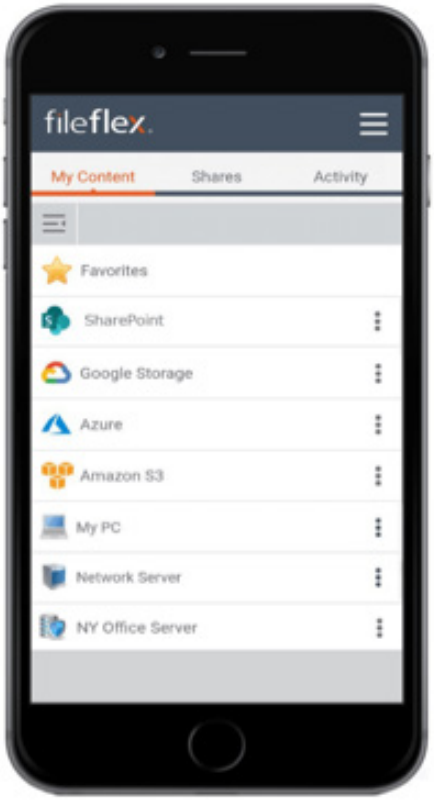
Le modèle «ne jamais faire confiance, toujours vérifier» qui sous-tend le système FileFlex permet aux utilisateurs de consulter leurs données depuis n'importe quel endroit et n'importe quel appareil sans compromettre la sécurité. Toute information et communication est stockée et protégée par un pare-feu de qualité industrielle pouvant également contrecarrer les interventions d'un tiers, peu importe la sophistication de leur technologie

Bien que nous nous attendons à ce que les échelons supérieurs du gouvernement canadien comme le Cabinet du Premier ministre (CPM), le Service canadien du renseignement de sécurité (SCRS) et le corps diplomatique (Bureau des affaires mondiales), utilisent, entre autres outils, les modèles E2EE et «Zero Trust», nous ne pouvons en être certain. Mais ce que nous savons, c'est que la majorité des chercheurs en médecine, des travailleurs de la santé et d'autres employés gouvernementaux n'ont jamais eu d'outils aussi sophistiqués puisqu'ils dépendent des réseaux informatiques locaux fournis par leurs agences gouvernementales ou ministères respectifs.

Avec plusieurs chercheurs en médecine et employés du gouvernement appelés à travailler à domicile, le gouvernement canadien pourrait adopter des solutions comme le chiffrement E2EE pour les courriers électroniques, les messages textes, et la téléphonie, et le système FileFlex afin de mieux protéger sa main-d'œuvre et ses données. Alors que certains travailleurs à distance se sentent quelque peu en sécurité lorsqu'ils utilisent un réseau privé virtuel, il est intéressant de noter que «d'ici 2023, 60 % des entreprises supprimeront de façon graduelle la plupart de leurs RPV destinés aux connexions à distance en faveur d'un modèle de vérification systématique "Zero Trust" — Gartner.

Au moment où notre planète fait face à une crise sans précédent, amplifiée par les campagnes de désinformation des États voyous, les autorités canadiennes et les dirigeants de l'industrie doivent collaborer pour protéger la santé du pays, ses données et son avenir. Nous croyons que seule une solution issue de la science et de la technologie est la réponse juste.

Figure 4: Demonstration of the FileFlex platform.



Source: SafeSwiss

Références

Adriano, L. (s.d.). « Expert: Phishing attacks against work-from-home employees are on the rise ». À consulter en ligne à : https://www.insurancebusinessmag.com/ca/news/ cyber/expert-phishing-attacks-against-workfromhome-employees-are-on-the- rise-217178.aspx

Beavers, O. (2020, 20 mars). « Pompeo says China, Russia, Iran are spreading disinformation about coronavirus ». À consulter en ligne à : https://thehill.com/policy/ national-security/488,659-pompeo-says-china-russia-iran-are-spreading-disinformation-about

Bradshaw, S. et Philip N. Howard. 2019. L'ordre mondial de la désinformation : Inventaire mondial des médias sociaux organisés de 2019 Manipulation. Document de travail

2019.2. Oxford, Royaume-Uni : Projet sur la propagande informatique.

Le secteur canadien de la santé risque de subir des cyberattaques alors que la crainte de COVID-19 se répand : CBC News (2020, 19 mars). « Canada's health sector at risk of cyberattacks as COVID-19 fear spreads: CSE ». À consulter en ligne à : https://www.cbc.ca/news/politics/ health-covid-cyberattack-pandemic-1.5502968

Cellan-Jones, R. (2020, 26 février). « Coronavirus: Fake news is spreading fast ». À consulter en ligne à : https://www.bbc.com/news/technology-51646309

Corfield, G. (2020, 20 mars). « Online face mask sales scams, 400% uptick of coronavirus phishing reports: Brit cops'; workload shifts online along with the nation's ». À consulter en ligne à : https://www.theregister.co.uk/2020/03/20 coronavirus_scam_reports_police_up_400pc/

Doffman, Z. (2019, 20 août). « New Cyberattack Warning For Millions Of Home Internet Routers: Report ». À consulter en ligne à : https://www.forbes.com/sites/ zakdoffman/2019/08/20/new-study-warns-guest-networks-open-millions-of- home-Internet-routers-to-cyberattack/#1dd9f08c664d

Emmott, R. (2020, 18 mars). « Russia deploying coronavirus disinformation to sow panic in West, EU document says ». À consulter en ligne à : https://ca.news.yahoo.com/ russia-feeding-disinformation-coronavirus-sow-092759812.html

Foxall, A. (2020, 19 mars). « Coronavirus conspiracies are a gift to Russia's disinformation machine ». À consulter en ligne à : https://www.telegraph.co.uk/politics/ 2020/03/19/coronavirus-conspiracies-gift-russias-online-disinformation/

Greenberg, I et K. Fomina. "La Russie dit qu'elle n'a pratiquement pas de cas de coronavirus. Les médecins disent le contraire. (2020, 20 mars). Consulté sur https://codastory.com/waronscience/russia-coronavirus-mistrust/

Jozwiak, R. (2020, 19 mars). « EU Monitors Say Pro-Kremlin Media Spread Coronavirus Disinformation ». À consulter en ligne à : https://www.rferl.org/a/eu- monitors-say-pro-kremlin-media-spread-coronavirus-disinformation/30495695.html

Lim, S. (2020, 10 février). Pourquoi la désinformation est un danger clair et présent lors de l'épidémie de coronavirus. Consulté sur https://www.thedrum.com/news/2020/02/10/why-misinformation-clear-and-present-danger-during-the-coronavirusoutbreak.

Paddon, D. (2020, 18 mars). « Fraudulent COVID-19 emails specifically target Canadians, security firm says ». À consulter en ligne à : https://www.thestar.com/ business/2020/03/18/fraudulent-covid-19-emails-specifically-target-canadians-security-firm-says.html

Pratt, M. K. (2018, 16 janvier). « What is Zero Trust? A model for more effective security ». À consulter en ligne à : https://www.csoonline.com/article/3247848/what-is- zero-trust-a-model-for-more-effective-security.html

Rosenbaum, E. (2020, 20 mars). « Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems ». À consulter en ligne à : https:/ www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to- hit-remote-work.html

SafeSwiss. Consulté sur https://safeswiss.com/

Sharton, B. R. (2020, 20 mars). « Will Coronavirus Lead to More Cyber Attacks? ». À consulter en ligne à : https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber- attacks

Thakkar, J. (2019, 4 novembre). Chiffrement de bout en bout : Le bon, le mauvais et la politique. Consulté sur https://www.thesslstore.com/blog/end-to-end-encryption-the-good-the-bad-and-the-politics/

Weinberg, Neal. "Le VPN est en train de mourir, vive la confiance zéro." Le monde des réseaux. Publié le 4 décembre 2019. Disponible en ligne à l'adresse https://www.networkworld.com/article/3487720/the-vpn-is-dying-long-live-zero-trust.html.

À propos de l'Institut des politiques du Nord

L'Institut des politiques du Nord est le groupe de réflexion indépendant de l'Ontario. Nous effectuons de la recherche, accumulons et diffusons des preuves, trouvons des opportunités en matière de politiques, afin de favoriser la croissance et la durabilité des collectivités du Nord. Nous avons des bureaux à Thunder Bay et Sudbury. Nous cherchons à améliorer les capacités du Nord ontarien de prendre l'initiative en politiques socioéconomiques qui ont des répercussions sur l'ensemble du Nord ontarien, de l'Ontario et du Canada.

Related Research

Connectivity in Northwestern Ontario: A House Digitally Divided Cannot
Rachel Rizzuto

En quoi l'accès à large bande peut jouer un rôle pour attirer de nouveaux venus
Christina Zefi

Distances physiques à longue distance : Travailler à domicile pendant le Covid-19
Sean Rosairo

Pour vous tenir au fait ou pour participer, veuillez communiquer avec nous :
1 (807) 343-8956 **info@northernpolicy.ca** **www.northernpolicy.ca/fr**

NORTHERN POLICY INSTITUTE | INSTITUT DES POLITIQUES DU NORD

northernpolicy.ca