I.T. SAFETY FOR KNOWN COVID-19 EXPLOITS

Presented by Quicktech

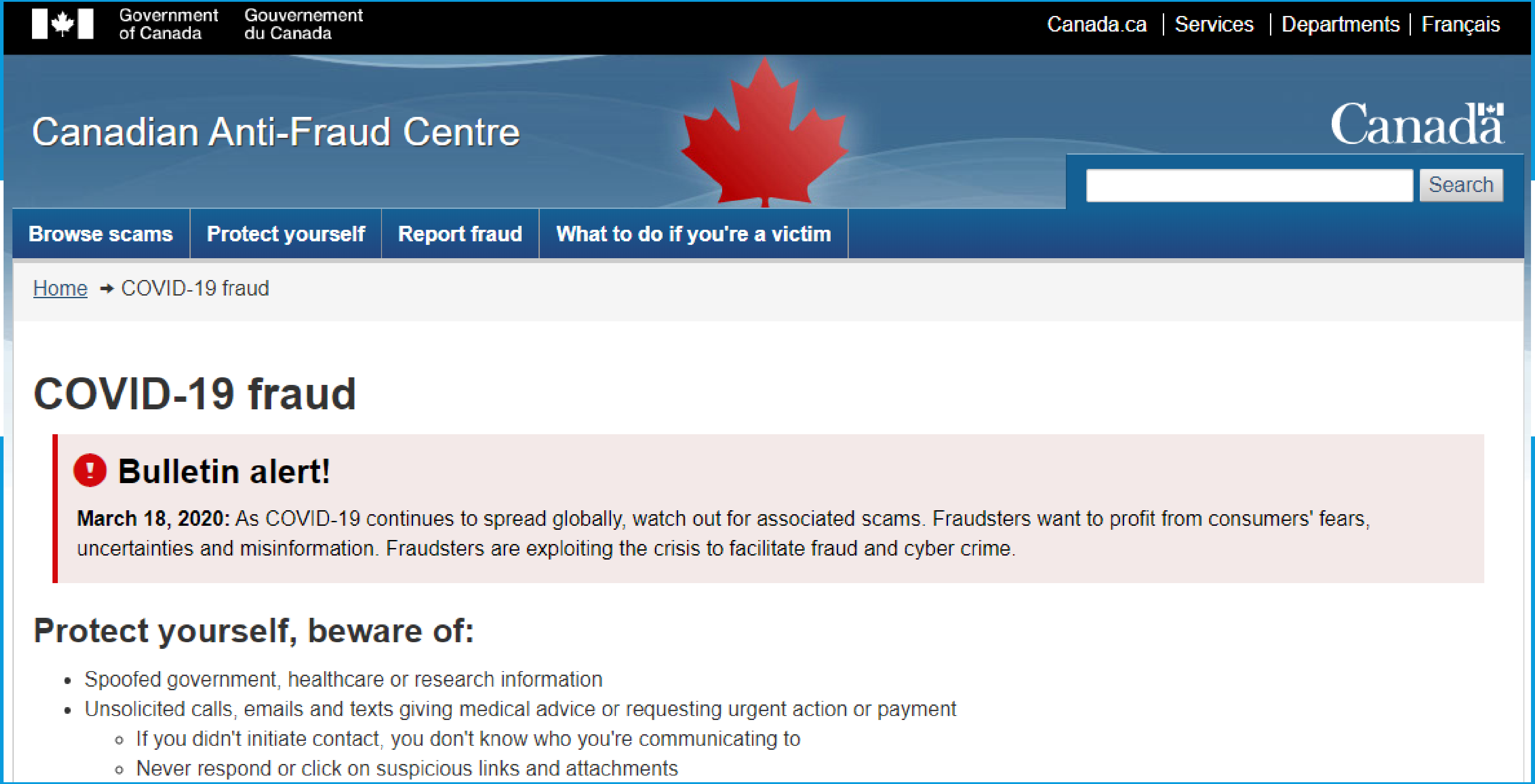
Introduction

This document is meant as an overview of the current landscape of known COVID-19 IT exploits, as well as the safety measures recommended by Quicktech, as well as the Canadian Government.

If you have any questions while reading through this document, please feel free to reach out to the Quicktech support team, at any time.

www.quicktech.ca
support@quicktech.ca
604.709.8324

Message From Canadian Anti-Fraud Center



Government of Canada
Gouvernement du Canada
Canada.ca | Services | Departments | Français
Canadian Anti-Fraud Centre
Canada
Search
Browse scams
Protect yourself
Report fraud
What to do if you're a victim

Home → COVID-19 fraud

COVID-19 fraud

Bulletin alert!

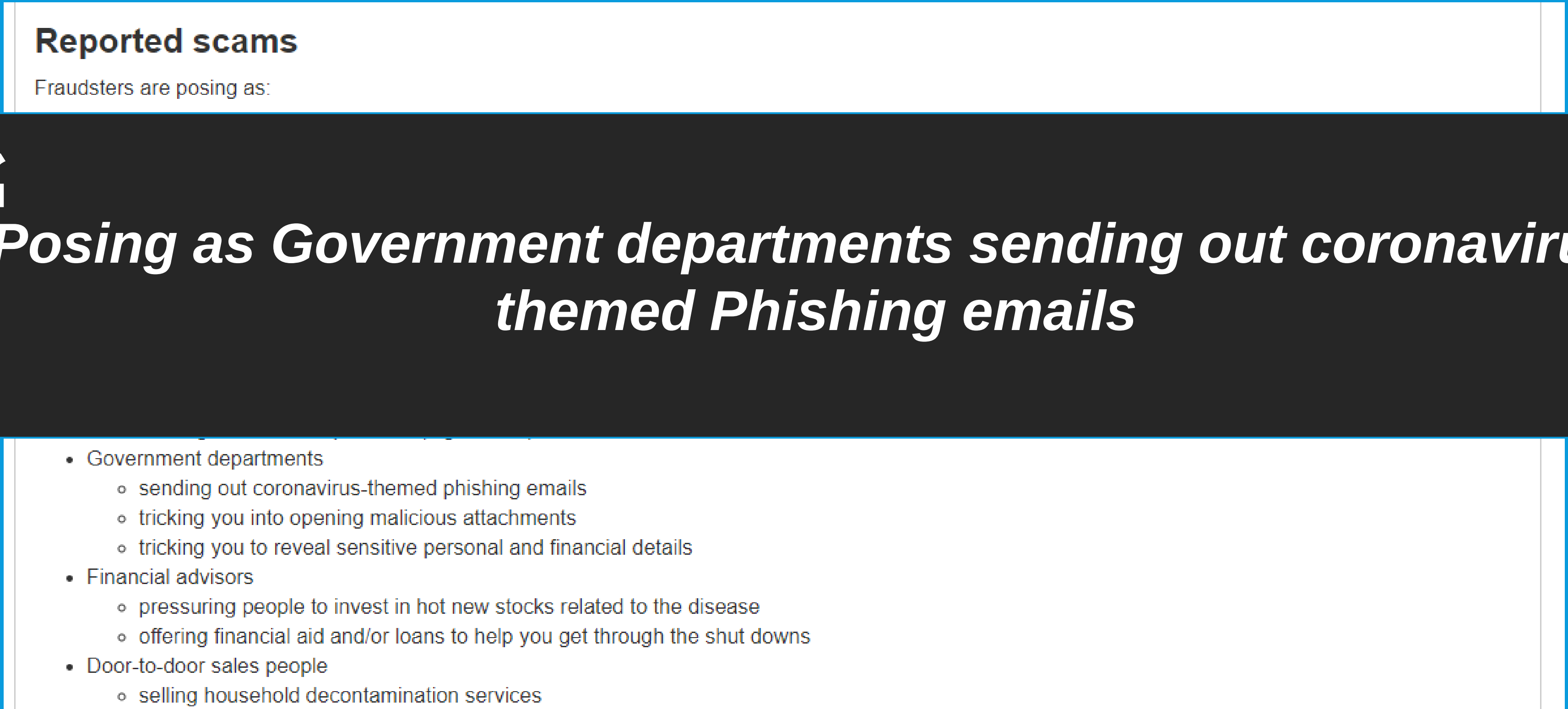
March 18, 2020: As COVID-19 continues to spread globally, watch out for associated scams. Fraudsters want to profit from consumers' fears, uncertainties and misinformation. Fraudsters are exploiting the crisis to facilitate fraud and cyber crime.

Protect yourself, beware of:

- Spoofed government, healthcare or research information
- Unsolicited calls, emails and texts giving medical advice or requesting urgent action or payment
  - If you didn't initiate contact, you don't know who you're communicating to
  - Never respond or click on suspicious links and attachments

https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

Message From Canadian Anti-Fraud Center



Reported scams

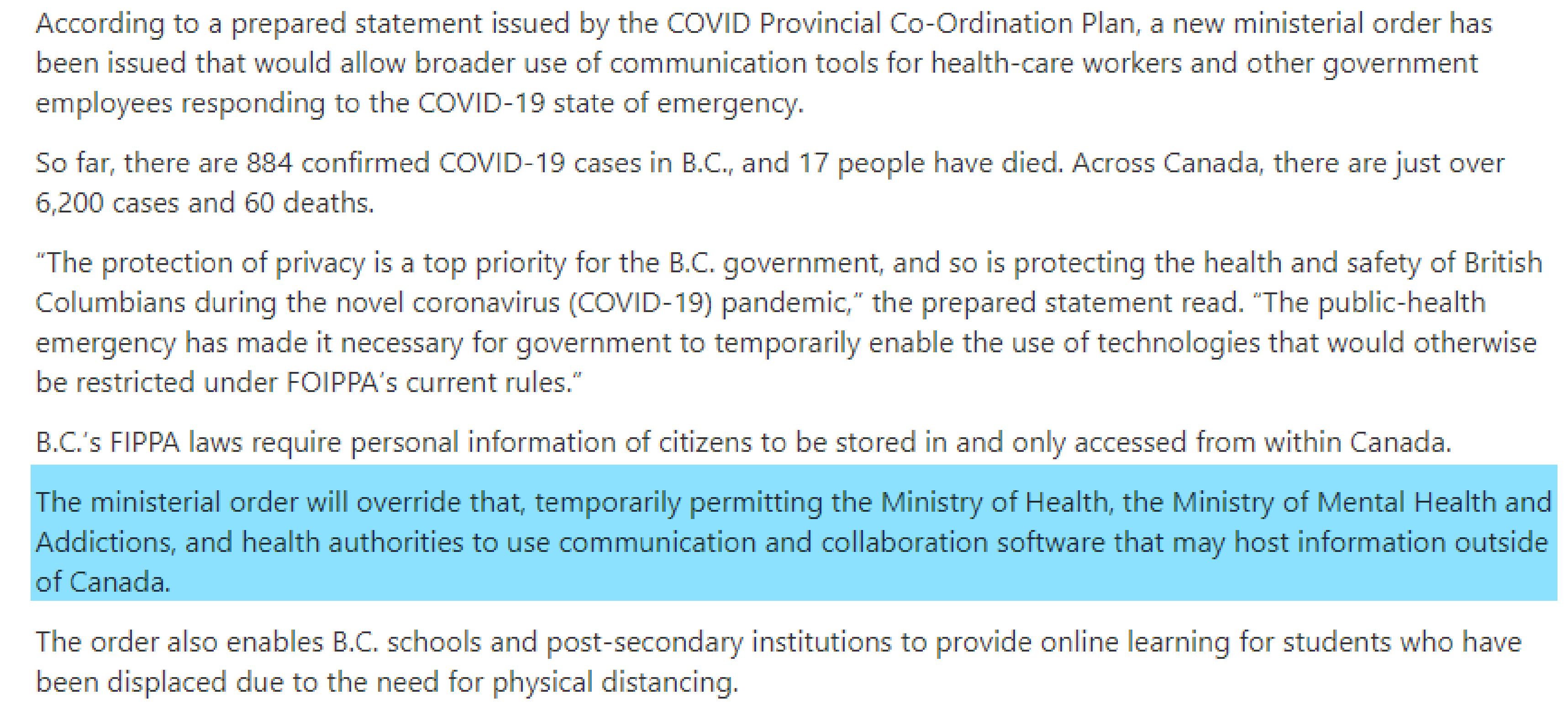
Fraudsters are posing as:

- Government departments
  - sending out coronavirus-themed phishing emails
  - tricking you into opening malicious attachments
  - tricking you to reveal sensitive personal and financial details
- Financial advisors
  - pressuring people to invest in hot new stocks related to the disease
  - offering financial aid and/or loans to help you get through the shut downs
- Door-to-door sales people
  - selling household decontamination services

> “
>
> ***Posing as Government departments sending out coronavirus-themed Phishing emails***

https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

Temporary FIPPA Changes In Response To COVID-19



According to a prepared statement issued by the COVID Provincial Co-Ordination Plan, a new ministerial order has been issued that would allow broader use of communication tools for health-care workers and other government employees responding to the COVID-19 state of emergency.

So far, there are 884 confirmed COVID-19 cases in B.C., and 17 people have died. Across Canada, there are just over 6,200 cases and 60 deaths.

“The protection of privacy is a top priority for the B.C. government, and so is protecting the health and safety of British Columbians during the novel coronavirus (COVID-19) pandemic,” the prepared statement read. “The public-health emergency has made it necessary for government to temporarily enable the use of technologies that would otherwise be restricted under FOIPPA’s current rules.”

B.C.’s FIPPA laws require personal information of citizens to be stored in and only accessed from within Canada.

The ministerial order will override that, temporarily permitting the Ministry of Health, the Ministry of Mental Health and Addictions, and health authorities to use communication and collaboration software that may host information outside of Canada.

The order also enables B.C. schools and post-secondary institutions to provide online learning for students who have been displaced due to the need for physical distancing.

TELEWORKING SAFETY

Security issues of teleworking

When you use business equipment outside of your organization’s IT security perimeters, it can create a weak link in your organization’s overall IT infrastructure. If it is not properly protected, these remote connections can be exploited by threat actors. It is important to protect your mobile devices, as well as any sensitive information and data—whether at rest or in transit. Threats can potentially jeopardize the confidentiality, the integrity and the availability of the information.

Teleworking risks

Be aware that teleworking increases the possibility of:

- Physical access to your device by unauthorized users
- Traffic manipulation (an attacker inserts their own traffic to influence data and obtain access to the mobile device or the organization’s network).
- Social engineering whereby threat actors trick you into sharing information or granting access to your device.
- Compromised login credentials, forgetting your password, weak security settings, etc.
- Compromised communications links through:
- Eavesdropping—an attacker listens to Wi-Fi or network traffic or records on-line activity. This can include capturing your username and passwords.

TELEWORKING SAFETY

Safeguards for Corporate Devices

- Use your device for work related matters only and not for personal use
- Do not install or configure software or hardware on your device
- Learn how to safely use the device issued to you
- Always follow your organization’s security policy and understand your security obligations
- Never connect an unencrypted USB key or other peripheral to your device
- Ensure that the information on your device is encrypted when at rest
- Follow your employers' data storage policies
- Always connect to your organization’s network using the provided equipment through a virtual private network (VPN)

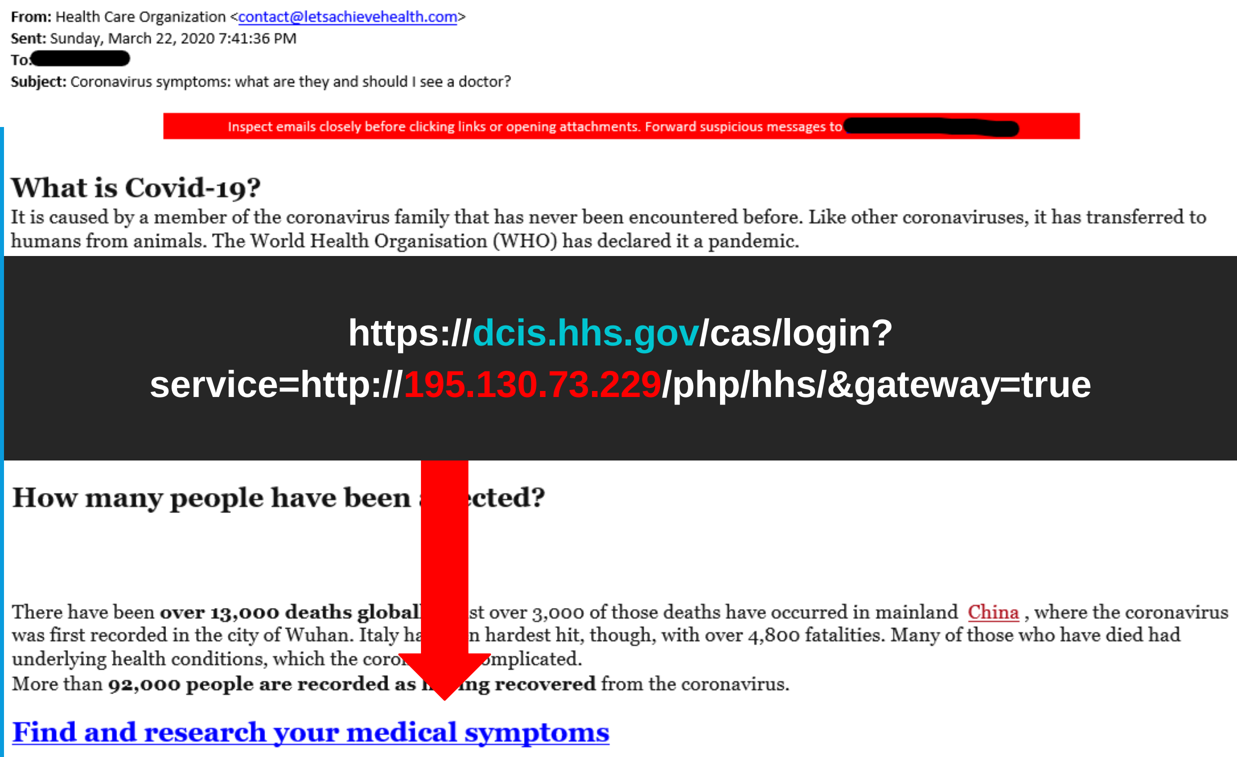
TELEWORKING SAFETY

Safeguards for Personal Devices

- Restrict computer use to you only
- Comply with business data storage policies, always store business data in approved cloud or local storage
- Ensure that your operating system and applications are receiving regular patch updates
- Secure your home wireless router with strong WPA2 passphrases
- Never use unapproved, unencrypted USB drives or portable hard drives to store business information.
- Use strong authentication such as public key infrastructure (PKI) or two-factor authentication, not just the traditional user-name and password
- Do not leave sensitive data which can be accessed or copied on an unsupervised computer
- Report suspicious, suspected and actual security events to your IT security team immediately

EXAMPLE: HHS EMAIL SPOOFING

- Phishing email providing COVID-19 information with a link from the Dept of Health and Human Services
- Clicking on link takes you to legitimate **hhs.gov** domain exposed to open redirect vulnerability
- Redirect leads to downloading information stealers made to scam credit cards, credentials, or browser data



From: Health Care Organization <contact@letsachievehealth.com>
Sent: Sunday, March 22, 2020 7:41:36 PM
To: [redacted]
Subject: Coronavirus symptoms: what are they and should I see a doctor?

Inspect emails closely before clicking links or opening attachments. Forward suspicious messages to [redacted]

What is Covid-19?

It is caused by a member of the coronavirus family that has never been encountered before. Like other coronaviruses, it has transferred to humans from animals. The World Health Organisation (WHO) has declared it a pandemic.

https://dcis.hhs.gov/cas/login?service=http://195.130.73.229/php/hhs/&gateway=true

How many people have been ▮cted?

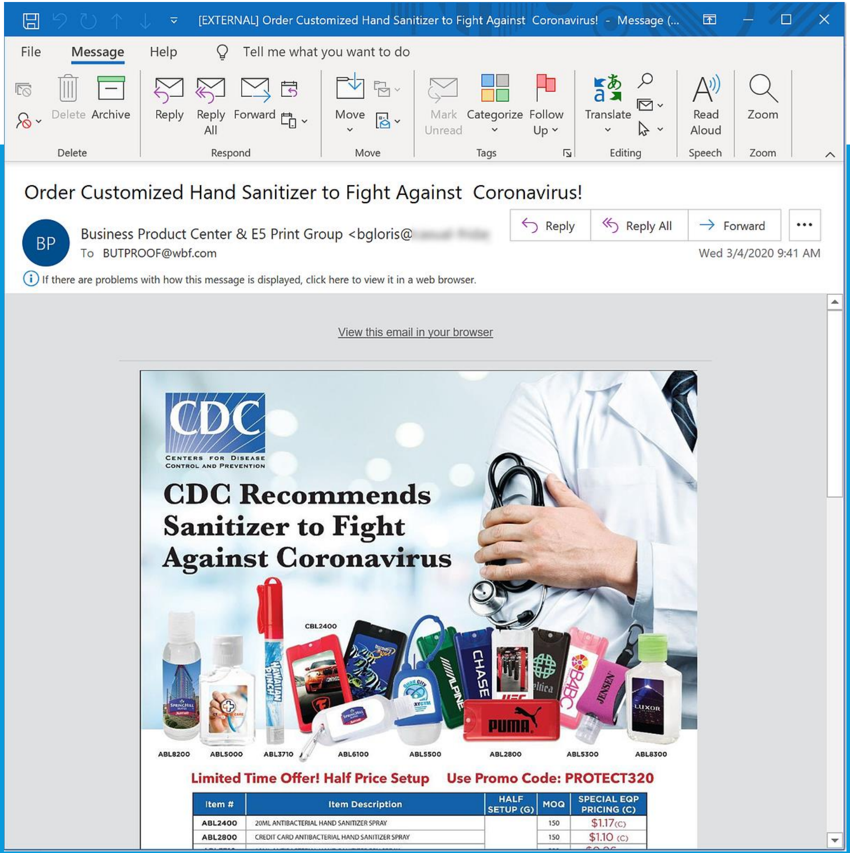
There have been **over 13,000 deaths global** st over 3,000 of those deaths have occurred in mainland China , where the coronavirus was first recorded in the city of Wuhan. Italy ha n hardest hit, though, with over 4,800 fatalities. Many of those who have died had underlying health conditions, which the coro omplicated.
More than **92,000 people are recorded as h ng recovered** from the coronavirus.

Find and research your medical symptoms

https://www.bleepingcomputer.com/news/security/hhsgov-open-redirect-used-by-coronavirus-phishing-to-spread-malware/

EXAMPLE: CDC EMAIL SPOOFING

- CDC and WHO remain among the most spoofed organizations during COVID-19 pandemic
- Clicking on links usually leads to credential stealing
- Higher quality polished advertisements
- Taking advantage of materials shortages, such as hand sanitizer



Order Customized Hand Sanitizer to Fight Against Coronavirus!

Business Product Center & E5 Print Group <bgloris@[redacted]

To BUTPROOF@wbf.com

Wed 3/4/2020 9:41 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

View this email in your browser

CDC Centers for Disease Control and Prevention

CDC Recommends Sanitizer to Fight Against Coronavirus

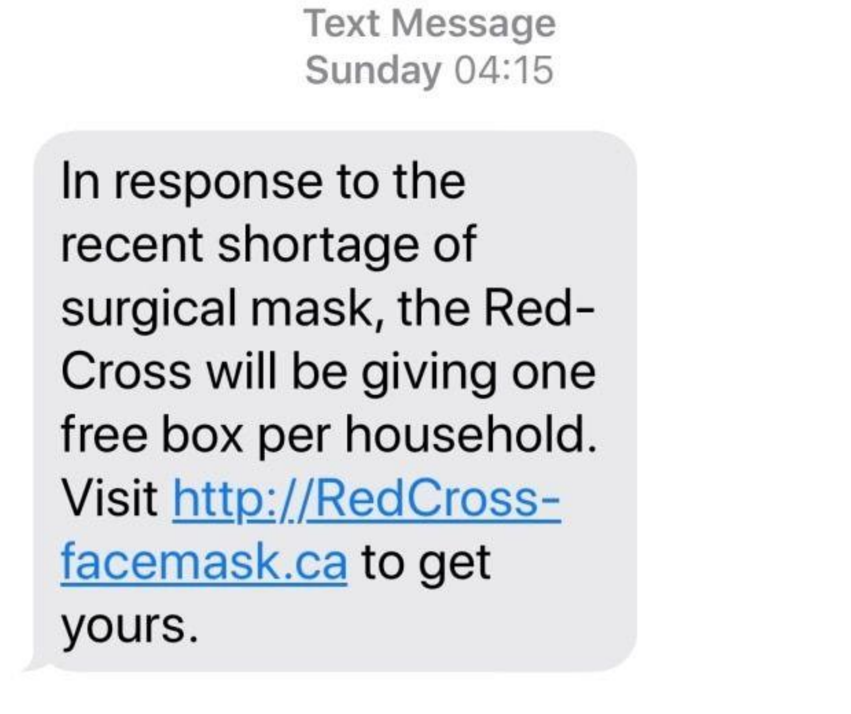
Limited Time Offer! Half Price Setup   Use Promo Code: PROTECT320

Item #	Item Description	HALF SETUP (G)	MOQ	SPECIAL EQP PRICING (C)
ABL2400	20ML ANTIBACTERIAL HAND SANITIZER SPRAY		150	$1.17(C)
ABL2800	CREDIT CARD ANTIBACTERIAL HAND SANITIZER SPRAY		150	$1.10 (C)

https://blog.knowbe4.com/exploiting-the-coronavirus-the-spammers-the-scammers-and-the-bad-guys

EXAMPLE: RED CROSS TEXT MESSAGE

- Attackers preying on shortage of personal protective equipment (PPE)
- Following this link, victims are asked to pay a “delivery fee” and provide credit card information



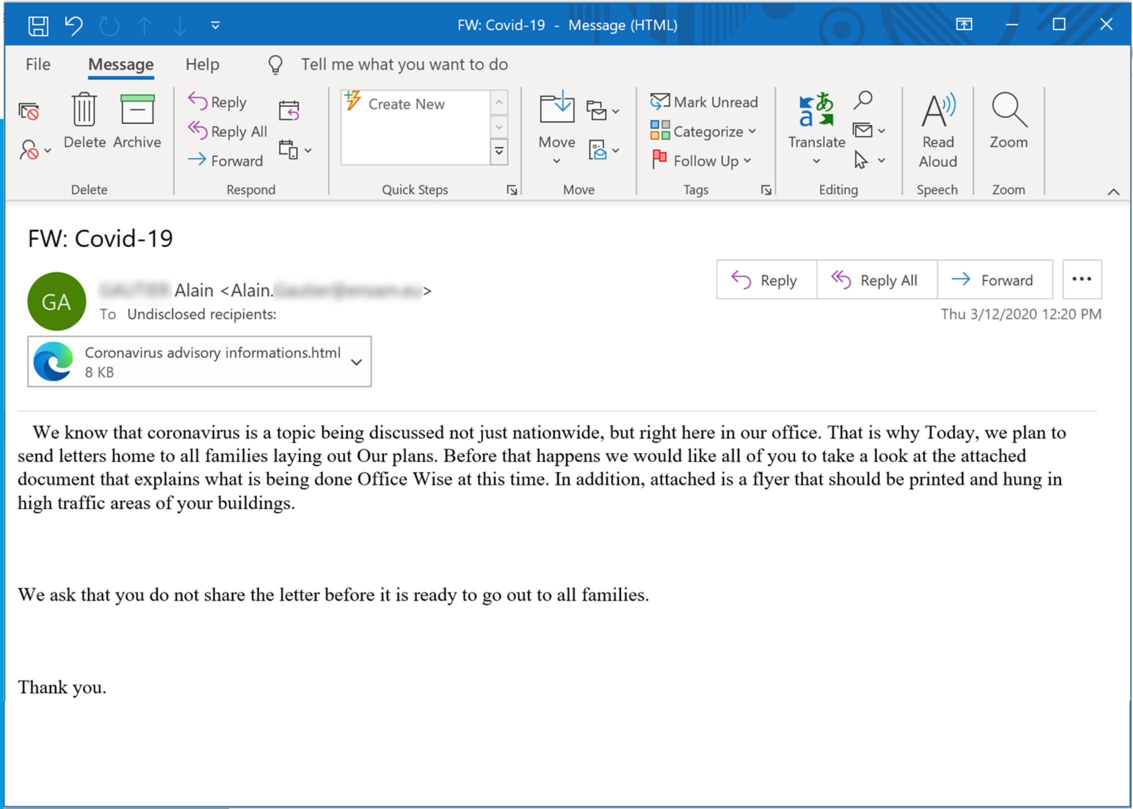
Text Message
Sunday 04:15

In response to the recent shortage of surgical mask, the Red-Cross will be giving one free box per household. Visit http://RedCross-facemask.ca to get yours.

https://nationalpost.com/news/beware-of-covid-19-scams-fraudsters-offer-free-masks-from-the-red-cross-or-fake-test-kits

EXAMPLE: SPOOFING INTERNAL HR

- Spoofing internal departments using vague and generic phrasing
- Fake "office plan" during COVID-19 asking to be reviewed and printed
- The attachment itself is actually credential stealing, requesting O365 credentials



FW: Covid-19

GA [redacted] Alain <Alain.[redacted]>

To Undisclosed recipients:

Thu 3/12/2020 12:20 PM

Coronavirus advisory informations.html
8 KB

We know that coronavirus is a topic being discussed not just nationwide, but right here in our office. That is why Today, we plan to send letters home to all families laying out Our plans. Before that happens we would like all of you to take a look at the attached document that explains what is being done Office Wise at this time. In addition, attached is a flyer that should be printed and hung in high traffic areas of your buildings.

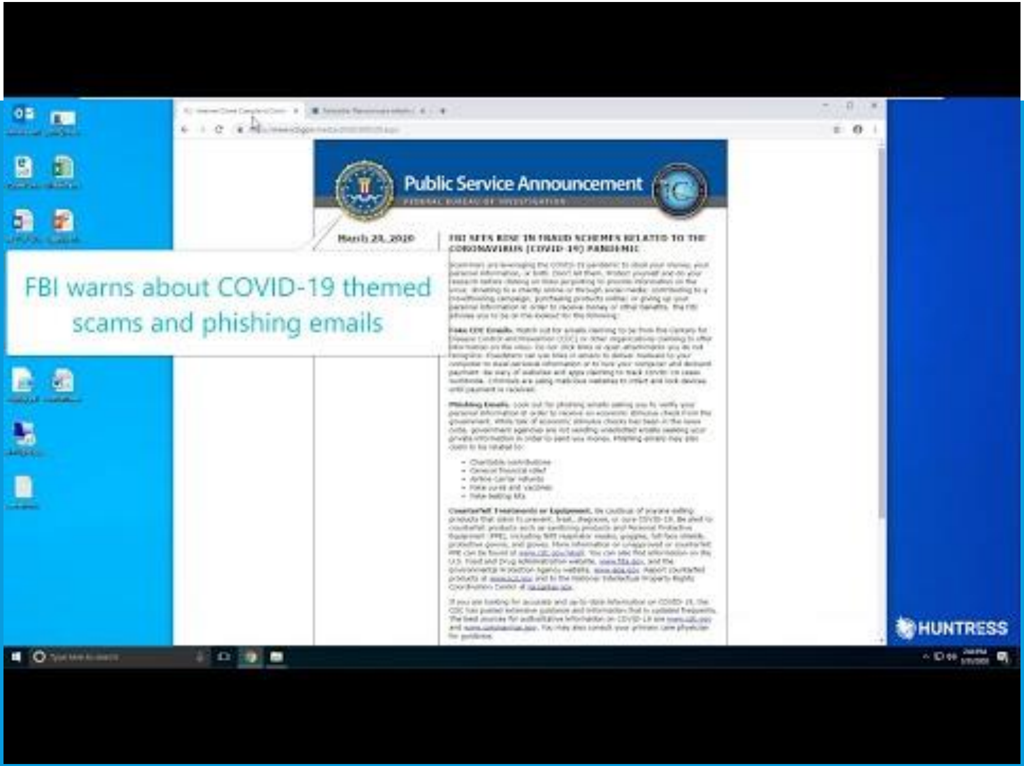
We ask that you do not share the letter before it is ready to go out to all families.

Thank you.

https://blog.knowbe4.com/extreme-measures-the-epidemic-of-covid-19-phishing-emails-rages-on

EXAMPLE: COVID-19 RANSOMWARE

- FBI warns of COVID-themed scams and phishing emails known to spread ransomware
- New Coronavirus phishing campaign attaches Netwalker ransomware file
- When executed, this ransomware encrypts files on the machine and attempts to spread to other Windows machines on the network



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 20, 2020

FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

[illegible]

FBI warns about COVID-19 themed scams and phishing emails

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/