

# Cybersecurity in the Era of COVID-19

08.05.2020

Jake van der Laan • CIO @ FCNB.CA

<https://www.linkedin.com/in/jakevanderlaan/>

jake.vanderlaan@fcnb.ca





# Outline

- What cybersecurity looked like as we entered 2020
- Impacts of COVID-19
- How to protect yourself while working from home



**Before COVID-19**





# Meta-analysis of Recent Reports

- Sophos 2020 Threat Report
- Infosec Top Cybersecurity Predictions for 2020
- Trend Micro Security Predictions for 2020
- World Economic Forum Cybersecurity Trends for 2020
- The Hacker News Top 5 Cybersecurity and Cybercrime Predictions for 2020
- Verizon Data Breach Investigations Report 2019
- Malwarebytes State of Ransomware Report 2019
- ISACA State of Cybersecurity Report 2019
- Symantec Internet Security Threat Report 2019
- Flexera 2020 State of the Cloud Report



# 1. Ransomware

- Still growing - focused on small and medium enterprises (SMEs)
- Primarily mediated through phishing and social engineering
- Exploiting remote management tools
- Increased sophistication
  - Prioritized encryption
  - Delayed activation - attacking backups first
- Intelligence gathering from breached/stolen data

## Categories:

Hosting

Forums

Private Sites

Communication

Hacking

Libraries/Wikis

Markets

Link Lists

Social

Other

Adult

Security

## GandCrab as a service Ransomware RaaS

106   3

Dashboard access official !. Features • Autodetected Bitcoin Payments • Auto Spread • Change Process Name • Change Ransom Amount • Command-and-control Center • Countdown Timer • Delete All Restore Points • Detects VM, Sandbox And Debugger Environments • Disable Regedit • Disable Safe Boot • Disable Shutdown • Disable Task Manager • Edit File Icon • Empty Recycle Bin • Enable USB Infection • Files On External Media Also Encrypted • Full Lifetime License • Fully Undetectable • Generate PDF Reports • GEO Map • Hide GandCrab Files • Master Boot Record Exploit • Military Grade Encryption • Multi Language • No Dependency • Payment Page Link • Quick File Encryption • Real Time Ticket Support System For Victims • Secure File Erase • Statistics • Text To Speech • UAC Exploit • Unlimited Builds • Weekly Updates.

<http://gandcr4cponzb2it.onion> Offline: GMT 2020-01-18 18:27:02

Please leave a rating!

Positive: ☐

Negative: ☐

Please add your name to your comment



## 2. Mobile

- Currently #1 attack vector
- Android focused
- 50% increase in credential stealing malware
- SIM jacking is up
- App “fleeceware” persistent
  - Data collection and privacy issues (who reads the EULA)
- Bring Your Own Device (BYOD) risks



## Unlock all features

Fortunemirror

**Starting today**

**3-day free trial**

**Starting Jan 9, 2020**

**\$69.99/week**

- The next step is to add a payment method
- Cancel anytime in Subscriptions on Google Play
- You won't be charged if you cancel before Jan 9, 2020
- We'll send you a reminder 2 days before your trial ends



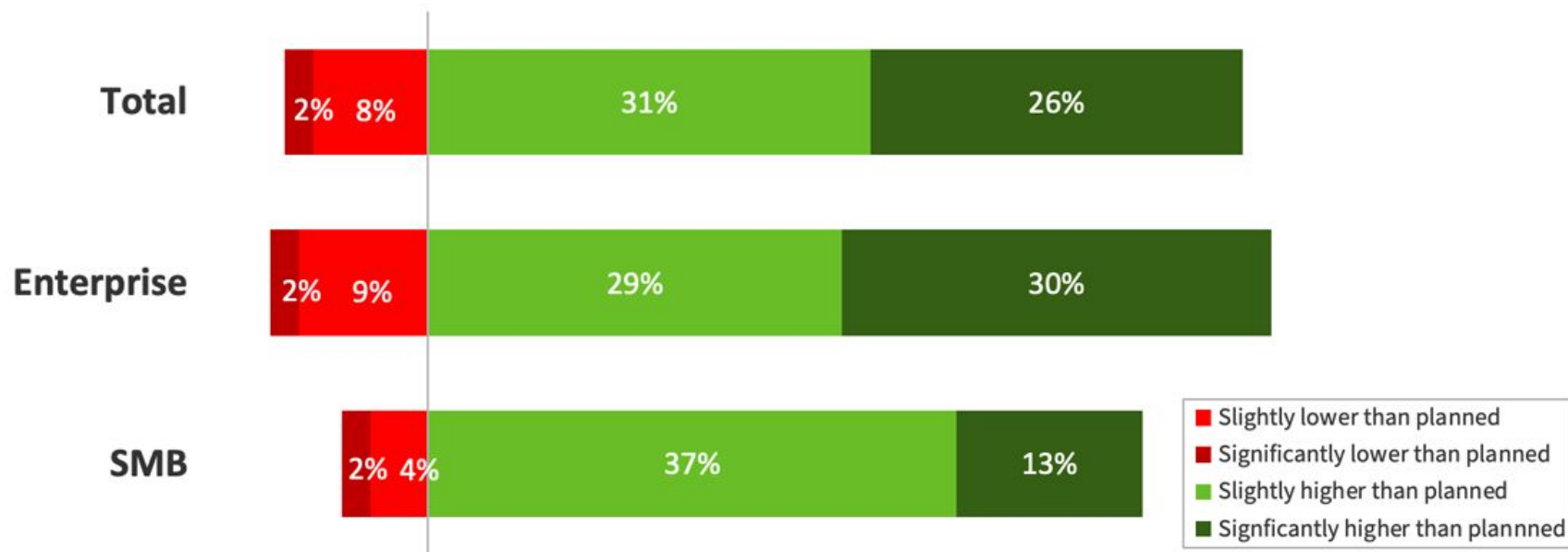


## 3. Cloud

- Misconfiguration risk - it's the consumer not the vendor
- Administrator's device control should be key priority
- End users training
- Unsecured third party users or dependencies

## Change from Planned Cloud Usage Due to COVID-19

% of respondents



N=187, asked only of later respondents

Source: Flexera 2020 State of the Cloud Report



## 4. Supply Chains and Third Parties

- The weakest link - attacks were up 70% in 2019
- Detection delay and visibility limitation risks
- Misplaced managed service provider (MSP) trust
- Regulatory requirements are lagging



## 5. Fintech and Open Data

- Online banking, ATMs and payments risks are growing
- Open banking - data harvest and misuse risks
- Security is simply not a priority with startups



## 6. Artificial Intelligence (AI)

- The ability to mimic legitimate activity is getting very good rapidly
- Supercharges social engineering, at scale
- Generative AI (e.g. “deepfakes”) enable more dangerous “wetware” attacks
- Automatic text interpretation and generation capabilities continue to get better and better
- AI based sandbox detection frustrates security systems

TECH ARTIFICIAL INTELLIGENCE

# AI deepfakes are now as simple as typing whatever you want your subject to say

24

*A scarily simple way to create fake videos and misinformation*

By James Vincent | Jun 10, 2019, 7:44am EDT

f t SHARE

## Adding New Words



Original Video



Synthetic Composite



Edited Video

I love the smell of ~~napalm~~ in the morning.  
french toast

## GOOD DEALS



Bang & Olufsen's excellent H9i headphones are cheaper than ever at Amazon





## 7. Advanced Persistent Threats (APTs)

- Opaque
- No international standards with which to address
- Bad guys are applying lessons learned
- Cyber “cold war” intensifying in today’s climate
- AI based mis-information attacks
- Critical infrastructure risks



## 8. Internet of Things (IoT)

- Billions of devices create many new attack surfaces
- Botnet risks
- Security by design not pervasive
- Patch deployment challenges
- 5G vulnerabilities (security by design v. first to market ... )
- Industrial control systems upgrade risks

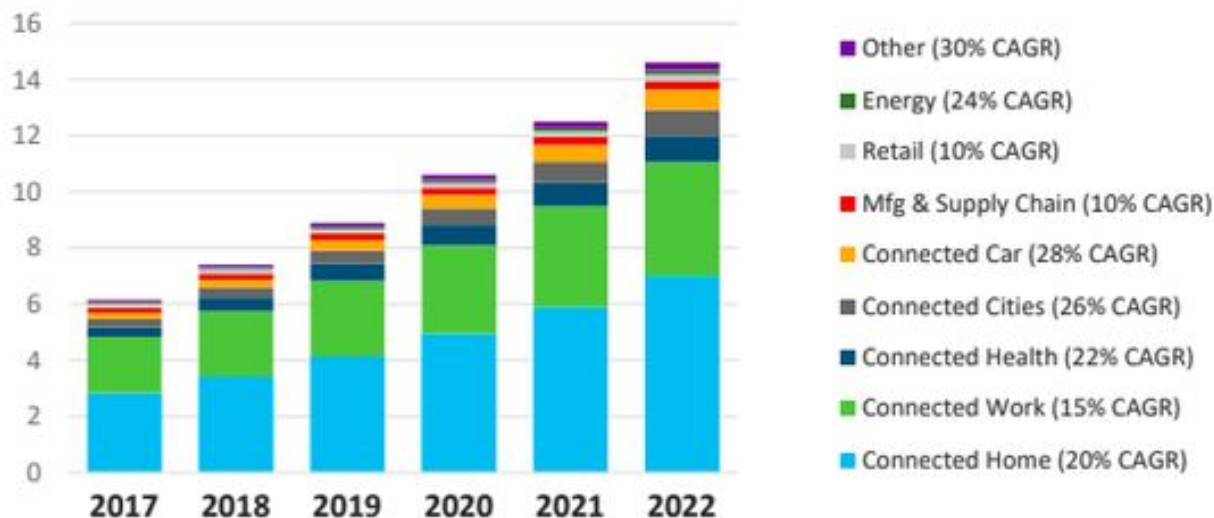


# Global M2M Connections / IoT Growth by Vertical

By 2022, connected home largest, connected car fastest growth

19% CAGR  
2017–2022

Billions of  
M2M  
Connections

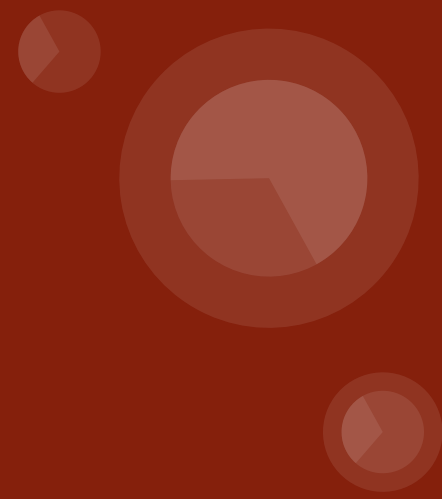




## 9. Other Developments and Issues

- Crime as a Service (CaaS)
- Evolving use of cryptocurrencies
- Maturity assessment and KPIs for cybersecurity
- Underfunding
- Skills resource gap
- Regulated compliance? - prescription or principles based?

# COVID-19 Impacts





# Government Response

- States of Emergency or other significant public health measures
- Online information dissemination and education
- Procurement of required supplies (Medicine, PPE, masks, etc.)
- Use of tracking apps (WeChat in China to identify potential contacts)
- Financial relief programs



# Organizational Impacts

- Addressing social distancing requirements at the workplace
- Inability to perform many functions “the old way”
- Heavily curtailed interaction with the public
- Economic effects
- Employee fear and uncertainty



# Organizational Responses

- Rapid establishment of remote working capabilities
- Increased reliance on IT systems and adoption of new tools
- Adaptation of organizational processes
- Changes in organizational supply chains and relationships with third parties
- Operational downsizing
- Employee support and communication



# Personal Impacts

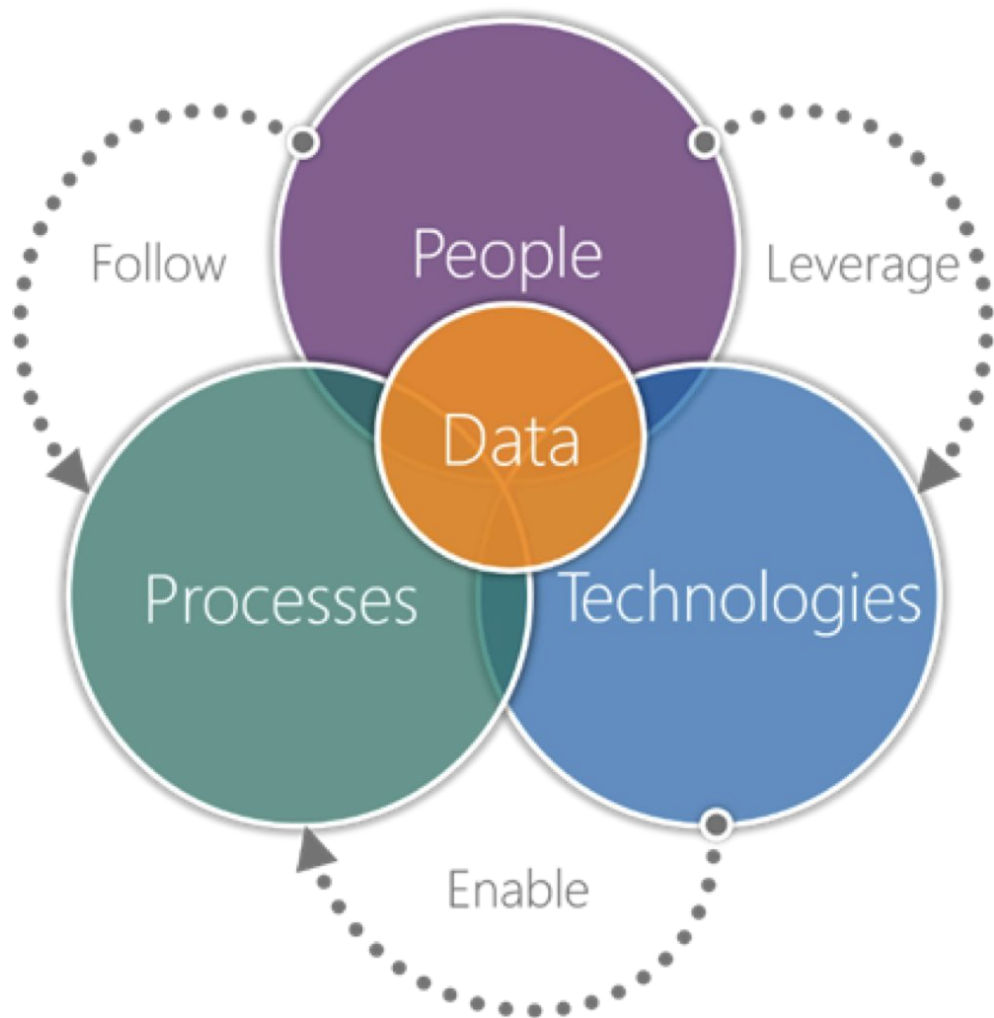
- Switch to a new work from home paradigm
- Anxiety over impacts of COVID-19 (health, financial)
- Interruption of social connections in and away from the office
- Distractions and pre-occupation while working from home

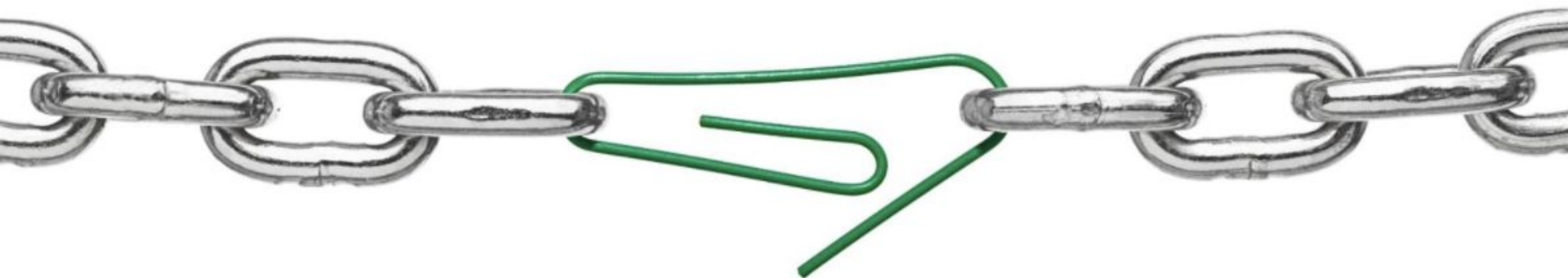


# Personal Responses

- Increased electronic interaction (email, chat, video, calls)
- Information seeking online
- Increased use of social media and new digital tools
- Alternative (online) sourcing of living needs
- Adjustment of financial profile (government support programs, loan deferrals, etc.)

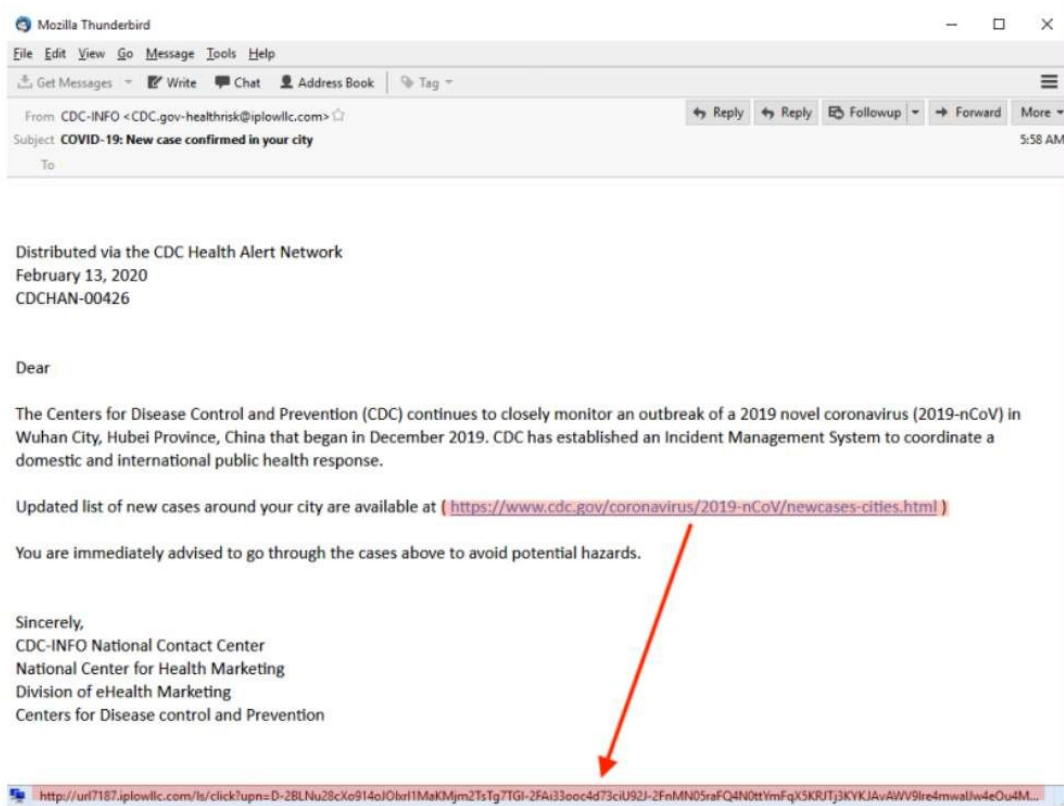






- Ah, Vous Dirai-Je, Maman
- Twinkle Twinkle Little Star
- The ABC Song
- Baa Baa Black Sheep

# Socially Engineering the Fear





# Fake Public Health Communications



Verify your account details to download the COVID-19 safety measures.

COVID-19 SAFETY PORTAL

## Login

To access your account, please enter your mobile phone number.

Phone Number:

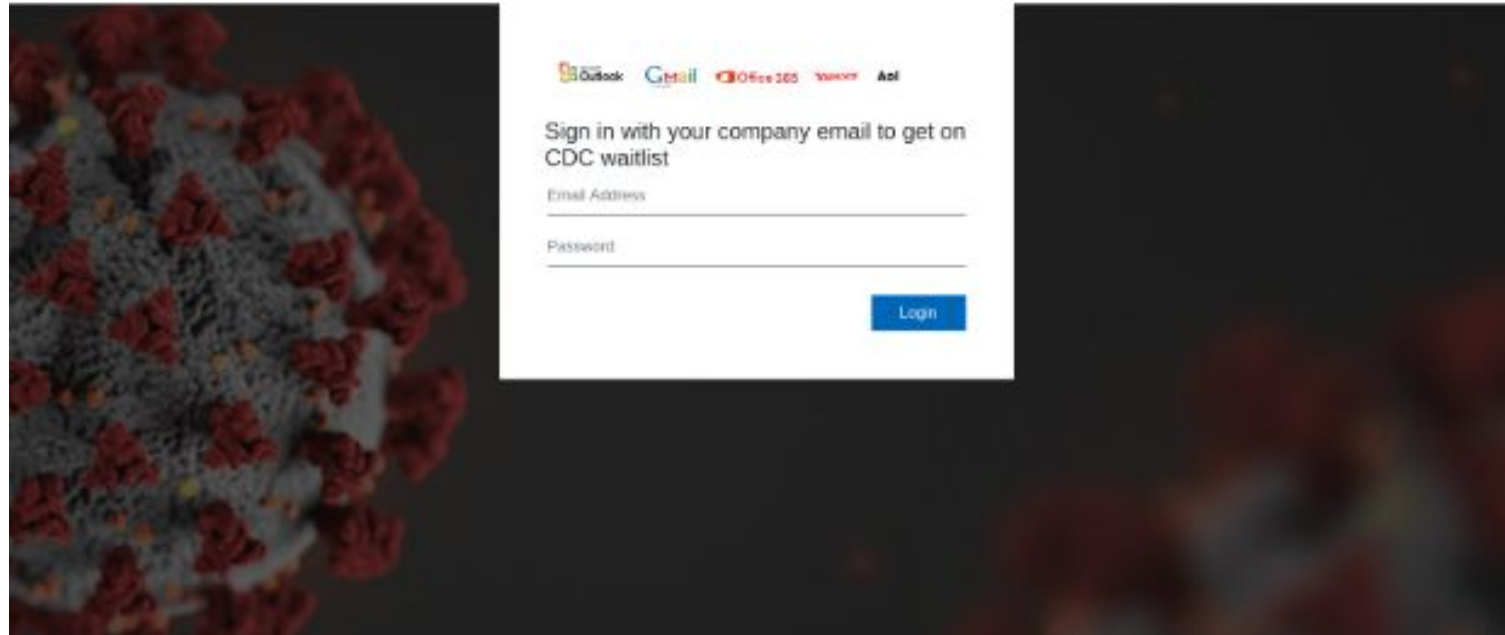
Email:

Password:

Verify

# Corporate Credentials Phishing

Centers for Disease Control and Prevention  
7: Saving Lives. Protecting People™



⌵

Home

# Explore

🔔 Notifications

✉ Messages

🔖 Bookmarks


📋 Lists

👤 Profile

⋮ More

Tweet


← Thread




MalwareHunterTeam

@malwrhunterteam

"Коронавірусна інфекція COVID-19.doc" (3 pages doc as by Ukraine's "Center for Public Health" or how it's in English, w/ macro) ->  
3b701eac4e3a73aec109120c97102c17edf88a20d1883dd5eef6db60d52b8d92  
Very interesting...  
🤔🤔  
[@VK\\_Intel](#) [@James\\_inthe\\_box](#)  
cc [@ItsReallyNick](#)





11:29 AM · Feb 22, 2020 · [Twitter Web Client](#)

26 Retweets 58 Likes

💬


↻

❤

🔗

Search Twitter

Relevant people




MalwareHunterTe...

@malwrhunterteam

Following

Official MHT Twitter account. Check out ID Ransomware (created by [@demonslay335](#)). Want to talk with us? DM [@0x7fff9](#) anytime. For more malwr tweets [@VK\\_Intel](#).




Vitali Kremes

@VK\_Intel

Follow

Ethical Hacker | Reverse Engineer | "Threat Seeker" by [@SCMagazine](#) | [keybase.io/vk\\_intel](#) | Head of Labs | Malware Course Author | Former: Government Cybercrime



James

@James\_inthe\_box

Follow

Trends for you

easter monday

health canada

spotify

#hamont

montreal

Show more

Terms

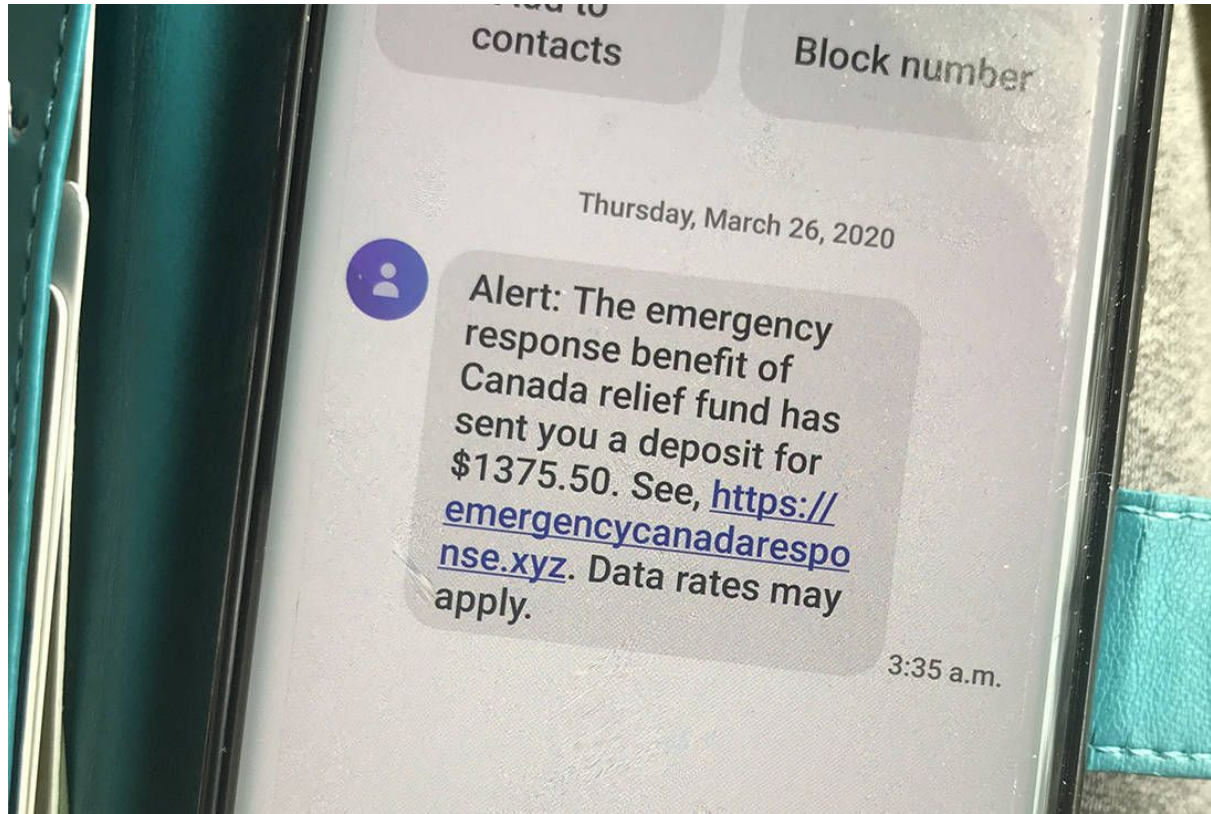
Privacy policy

Cookies

Ads info

More

# Financial Relief Smishing



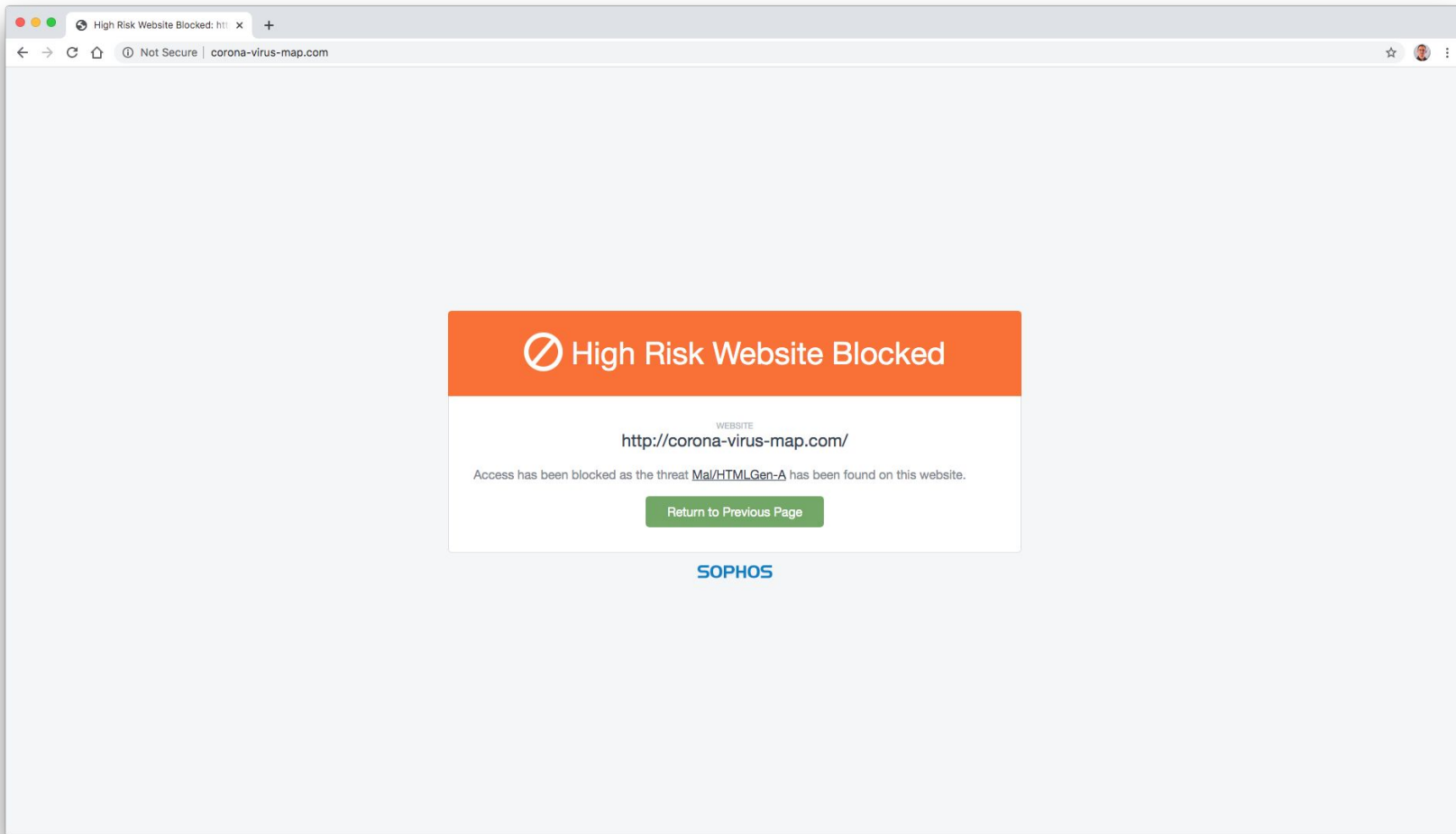




# Spreading Malware via Maps

Corona-Virus-Map.com





Late last month, a member of several Russian language cybercrime forums began selling a digital Coronavirus infection kit that uses the Hopkins interactive map as part of a Java-based malware deployment scheme. The kit costs \$200 if the buyer already has a Java code signing certificate, and \$700 if the buyer wishes to just use the seller's certificate.

“It loads [a] fully working online map of Corona Virus infected areas and other data,” the seller explains. “Map is resizable, interactive, and has real time data from World Health Organization and other sources. Users will think that PreLoader is actually a map, so they will open it and will spread it to their friends and it goes viral!”

<https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/>



# Mobile Device Malware

for android users: to get real-time number of coronavirus cases based on your GPS location please download the [mobile app version](#) of the website and enable "accurate reporting" for best experience

Thank you Reddit for the [incredible feedback](#). I will be implementing your suggestions as the week progresses. Stay tuned!

DASHBOARD

## United States Coronavirus (COVID-19) Tracker

Infection Map ([hide](#))

Sorry, we couldn't accurately determine your location. Please try reloading the page, or interact with the map manually instead.

Inform your friends & family:



Share



Share



Email



Tweet



Share



Buy me a coffee



Nationwide Live Data (refresh for updates)



Activate lock screen to get instant alert  
when a coronavirus patient is near you

ACTIVATE



Enable app in Accessibility for active  
stats monitoring

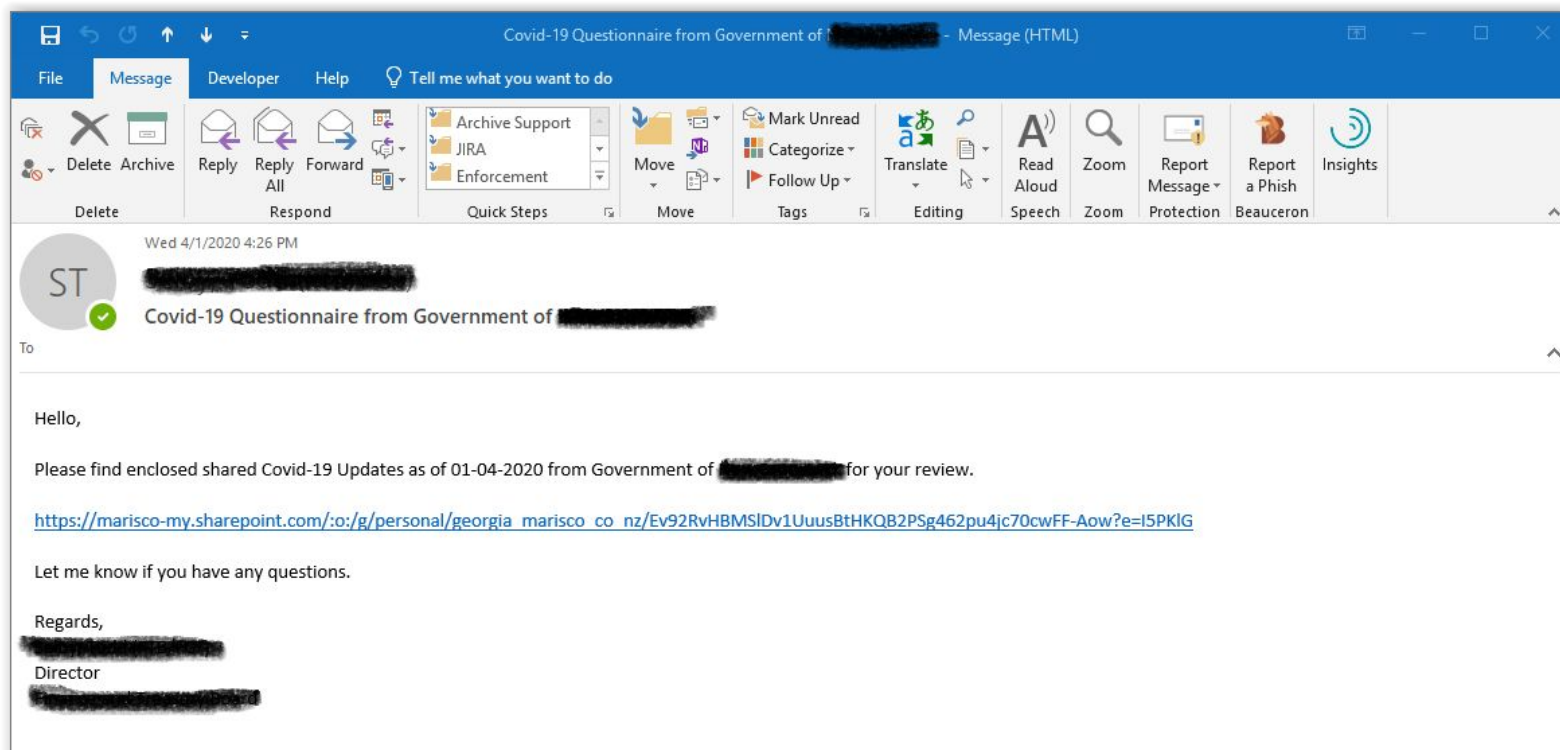
GRANT



SCAN AREA FOR CORONAVIRUS



# Hacked Internal Account Phishing



# Keylogger Malware

The screenshot shows a web browser window with the Bitdefender blog. The browser's address bar displays the URL: `hotforsecurity.bitdefender.com/blog/spammers-use-coronavirus-message-to-deploy-keylogger-22444.html`. The page features a dark, cyber-themed header with a glowing shield icon and the text "Cyber protection" and "HOT FOR SECURITY powered by Bitdefender". Below the header is a navigation bar with links: HOME, THREATS, SMART HOME SECURITY, DIGITAL PRIVACY, WORK FROM HOME: SAFETY TIPS, THE ABC OF CYBERSECURITY, and SECURITY VIDEOS. The main content area displays a blog post by Silviu STAHIE (@thesilviu) titled "Spammers Use Coronavirus Message to Deploy Keylogger", dated 1 month ago and 2 minutes read. The post's featured image shows a blue background with glowing purple spheres. To the right of the article is a social media sharing section with icons for Facebook (1.3M fans), Twitter (99.3K followers), RSS (2.7K subscribers), and YouTube (13 subscribers). Below this is a "RECENT SHOUTS" section with a link to "Meurig Parri on Microsoft Ends Support for Windows 7. What You Need to Know".

Spammers Use Coronavirus Message to Deploy Keylogger

Silviu STAHIE  
@thesilviu

1 month ago 2 Min Read

Share This!

INDUSTRY NEWS

**PROMO**

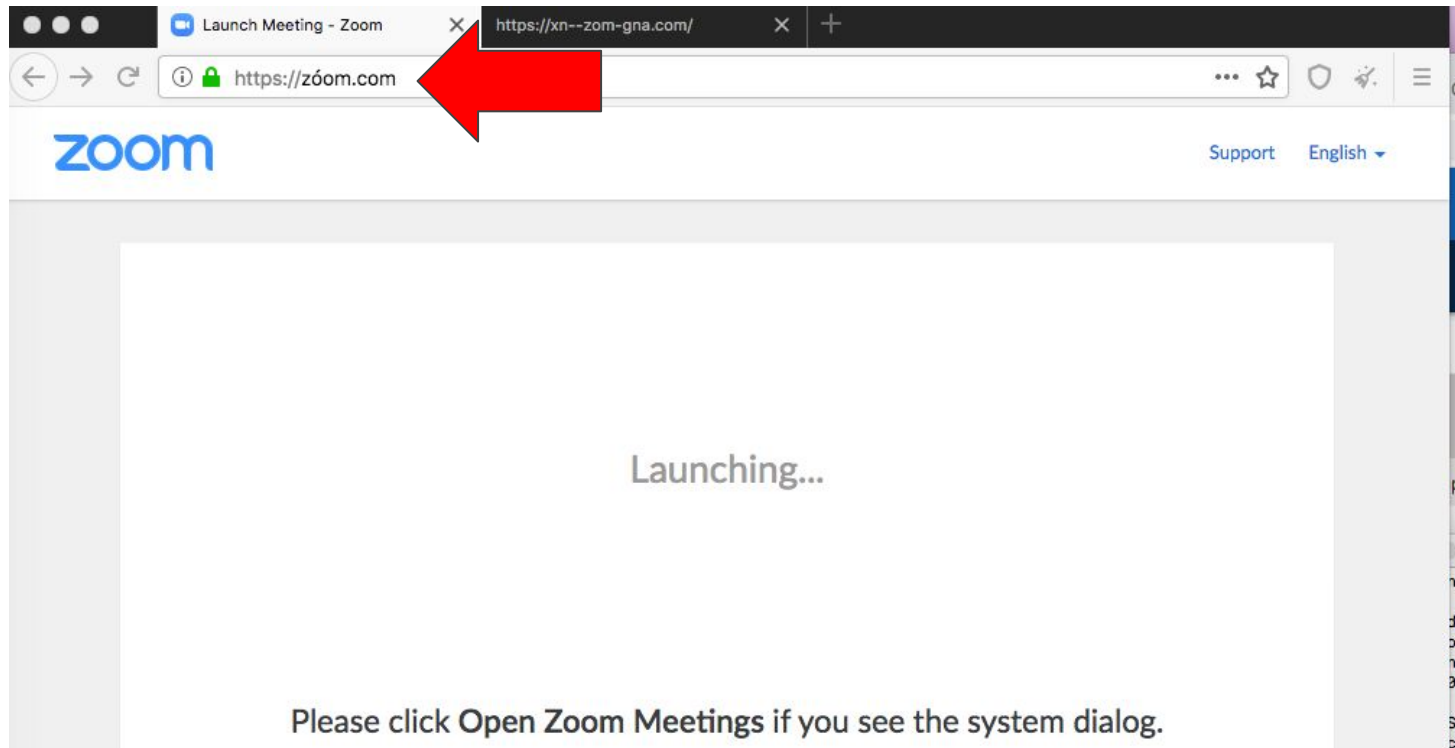
f 1.3M FANS	t 99.3K FOLLOWERS	📡 2.7K SUBSCRIBERS
📺 13 SUBSCRIBERS	❤️ 1.4M FANS LOVE US	

**RECENT SHOUTS**

- Meurig Parri on Microsoft Ends Support for Windows 7. What You Need to Know

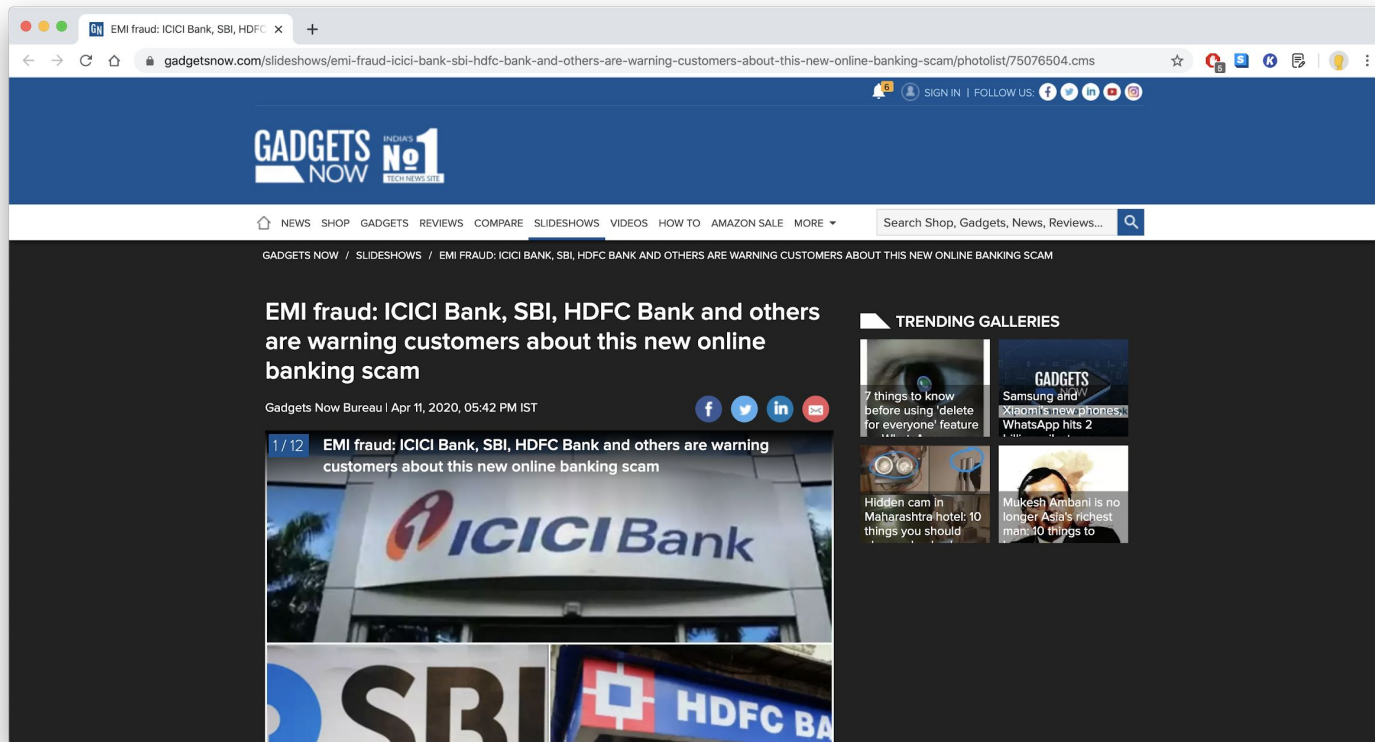


# Fake Video Conferencing Sites





# Bank Loan Deferral Phishing Scams





# Fraudulent Fundraising

HELP STOP CORONA-VIRUS - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From World Health Organization <mmarin@granollers.cat> ☆

Subject **HELP STOP CORONA-VIRUS**

2020-03-17, 6:19 p.m.

--

Dear Sir/Madam,

The Covid-19 Solidarity Response Fund is a secure way for individuals, philanthropies and businesses to contribute to the WHO-led effort to respond to the pandemic. The United Nations Foundation and the Swiss Philanthropy Foundation have created the solidarity fund to support WHO and partners in a massive effort to help countries prevent, detect, and manage the novel coronavirus – particularly those where the needs are the greatest.

The fund will enable us to:

1. Send essential supplies such as personal protective equipment to frontline health workers
2. Enable all countries to track and detect the disease by boosting laboratory capacity through training and equipment.
3. Ensure health workers and communities everywhere have access to the latest science-based information to protect themselves, prevent infection and care for those in need.
4. Accelerate efforts to fast-track the discovery and development of lifesaving vaccines, diagnostics and treatments.

The Strategic Preparedness and Response Plan outlines a funding need of at least US\$675 million for critical response efforts in countries most in need of help through April 2020. As this outbreak evolves, funding needs are likely to increase.

Reply to this email now to donate to the COVID-19 Response Fund through our secure digital wallet. You can find information there on payment options and tax exemption possibilities for some countries. Help save lives!

Dr. Tedros Adhanom Ghebreyesus  
Director General  
World Health Organization (WHO)

# Healthcare and Research Org Attacks

COVID-19 Vaccine Test Center

forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#5f7a5df518e5

Forbes

Billionaires Innovation Leadership Money Business Small Business Lifestyle Lists Advisor Featured Breaking More

EDITORS' PICK | 160,336 views | Mar 23, 2020, 06:10am EDT

## COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online

 **Davey Winder** Senior Contributor  
Cybersecurity  
*I report and analyse breaking cybersecurity and privacy stories*



A vaccine-testing facility is the latest to be hit by cyber-attackers

A medical facility on standby to help test any coronavirus vaccine has been hit by a ransomware group that promised not to target medical



ADVERTISEMENT



# Coronavirus: Cybercriminals target healthcare workers with email scam

Victims receive an email purportedly from the IT team with the subject "ALL STAFF: CORONA VIRUS AWARENESS", including a link.



Rowland Manthorpe

Technology correspondent @rowlsmanthorpe

🕒 Friday 13 March 2020 05:59, UK

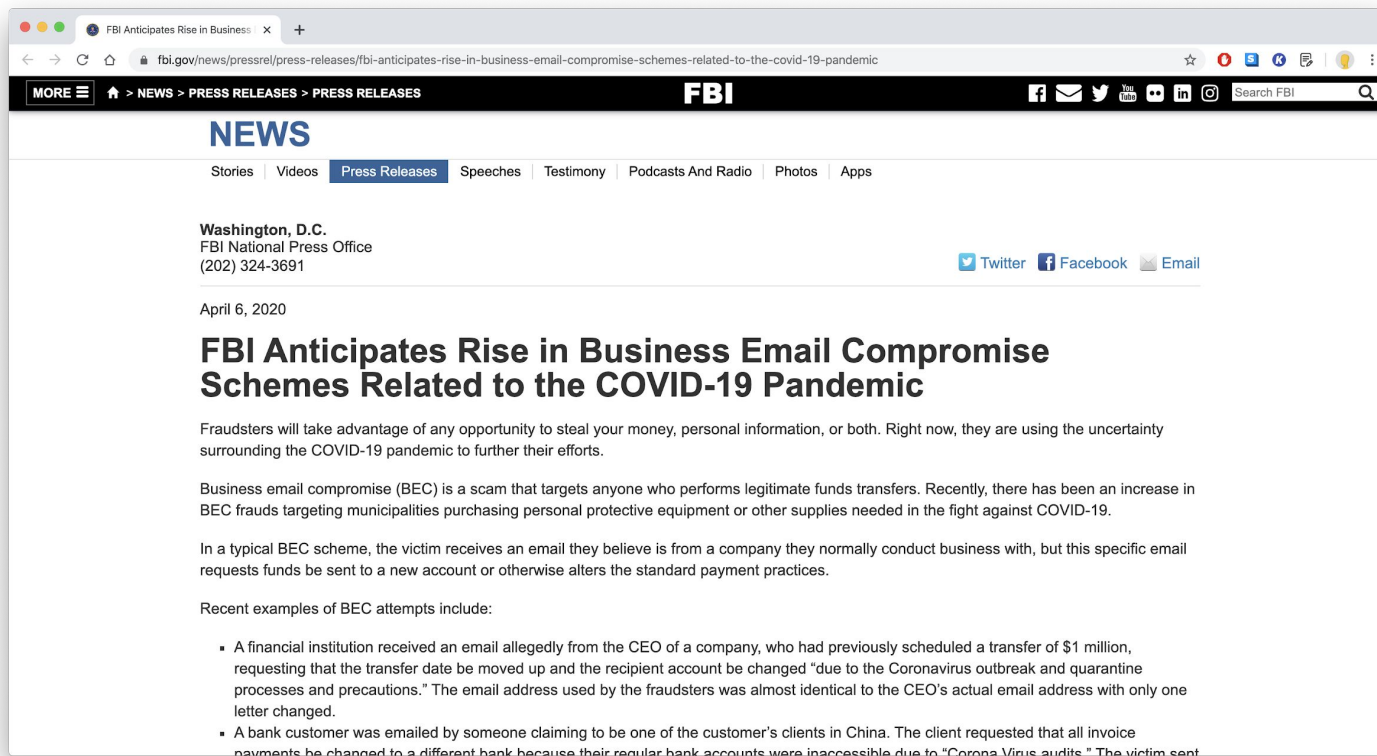
COVID-19

CORONAVIRUS

CYBERATTACKS



# COVID-19 based BEC attacks



The screenshot shows a web browser displaying the FBI's press release page. The browser's address bar shows the URL: [fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic](https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic). The page header includes the FBI logo and navigation links for News, Press Releases, Speeches, Testimony, Podcasts And Radio, Photos, and Apps. The main content area features the title "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic" and a sub-header "Washington, D.C. FBI National Press Office (202) 324-3691". The date "April 6, 2020" is displayed below the sub-header. The body of the press release begins with a paragraph stating that fraudsters will take advantage of the uncertainty surrounding the COVID-19 pandemic to steal money, personal information, or both. It then defines Business Email Compromise (BEC) as a scam targeting anyone who performs legitimate funds transfers. The text continues to describe a typical BEC scheme and provides recent examples of BEC attempts, including a financial institution receiving an email from a CEO and a bank customer being emailed by someone claiming to be a client in China.

**Washington, D.C.**  
FBI National Press Office  
(202) 324-3691

April 6, 2020

## FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic

Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts.

Business email compromise (BEC) is a scam that targets anyone who performs legitimate funds transfers. Recently, there has been an increase in BEC frauds targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19.

In a typical BEC scheme, the victim receives an email they believe is from a company they normally conduct business with, but this specific email requests funds be sent to a new account or otherwise alters the standard payment practices.

Recent examples of BEC attempts include:

- A financial institution received an email allegedly from the CEO of a company, who had previously scheduled a transfer of \$1 million, requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." The email address used by the fraudsters was almost identical to the CEO's actual email address with only one letter changed.
- A bank customer was emailed by someone claiming to be one of the customer's clients in China. The client requested that all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to "Corona Virus audits." The victim sent

# Medication Website Phishing

FIG. 1: # of Possible Drug-Related Phishing Domains (\*)

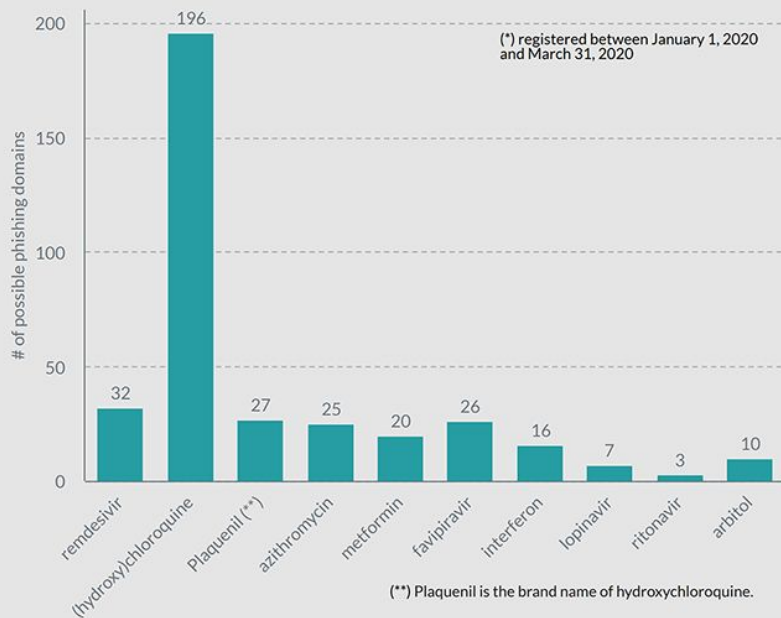
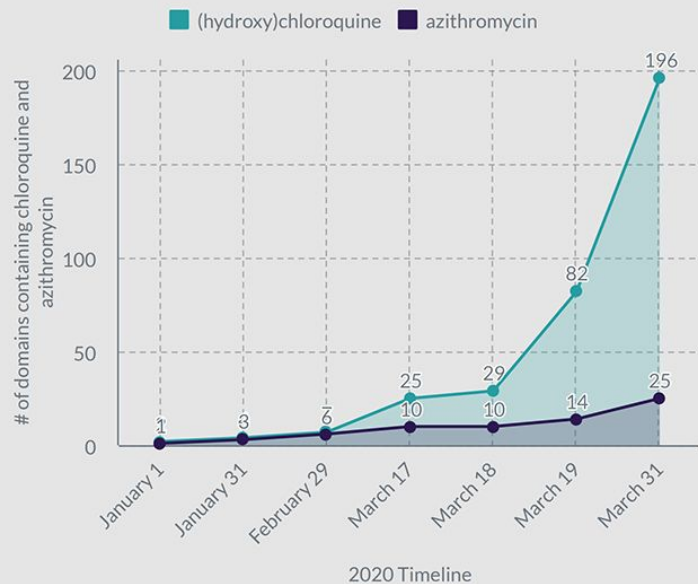


FIG. 2: # of Possible Drug-Related Phishing Domains





# An “Infodemic” of Fraudulent Websites

- **100,000+** .COM new domains containing COVID, CORONAVIRUS, PANDEMIC, since 1 January 2020
- Pro Privacy list of **160,000+** risky domains
- **2,000+** .CA domains



# Corona Antivirus — World's best protection

Download our AI Corona Antivirus for the best possible protection against the Corona COVID-19 virus.

[Download Corona Anti-Virus](#)







# **Working from Home Securely**





# Organizational Preparation

- Review and adapt remote working capabilities (laptops, VPN (can you handle the extra connections?), mobile phones)
- Consider cloud storage options (with 2FA)
- Create or review a Work from Home Policy
- Arrange or update cybersecurity awareness training
- Identify processes which require adaptation with staff working from home (**IT support**, **HR**, financial, procurement)



# Preparing to Work from Home

- What things do I need from the office to work effectively from home?
- What resources will be difficult to access? Is there a way to fix this?
- What (potential) corporate process changes may affect my work?
- Are my devices up to date? (they may need to be connected to your network to complete updates)



# The Work from Home Space

- Find a space where you can work without being disturbed
- Keep others away from this space
- Secure your devices and any documents when you are not in this space
- Find your WFH daily pattern (with breaks)



# The Home Network

- Ensure sufficient bandwidth
- Secure and update your router (see links on resource page)
  - Read the manual
  - Set a strong admin password
  - Ensure at least WPA-2 security is enabled
  - Change the SSID name and hide it if possible
  - Use MAC address filtering, if available
- Consider disabling certain IoT devices (Alexa, Google Home, etc.)
- Keep IoT devices on a separate network
- Ensure other users on the network are not putting connected devices at risk



# Devices

- Use only work provided devices for work
- Do not allow others (spouse, kids, friends) to use your devices
- Use a VPN
- Enable two-factor authentication if possible
- Keep them up to date



# Communication

- Set your online status
- Over communicate and use different modalities together (e.g. e-mail and chat, screen share and video)
- Use a headset if available
- Keep the personal away from the professional. In particular, don't use work email accounts for social media services (added bonus: any social media based phishing emails to your work account are thus always fake and easy to spot)



# Video and Audio Conferencing

- Test and understand your technology
- Screen share carefully
- Set a separate ID for each meeting
- Use a meeting room password or a waiting room
- Do not publicly post the meeting ID or connection details
- Do not enable “allow join before host” features
- Consider “locking” a meeting once all attendees have joined
- Explain core technology features and expected conduct to attendees before starting





# Be Proactive and Vigilant

- Use strong and unique passwords
  - Follow the three words-identifier-oddstuff paradigm, e.g.
    - stonecoffeepanFacebook432&
    - stonecoffeepanGoogle432&
- **Stop**, **look** and **think**, before you click that link
  - Be extra careful with emails with embedded links from inside your organization
- Be wary of COVID-19 “pre-texting” - be skeptical and verify
- Reach out to others in your organization to confirm high risk communications (financial approvals, account resets, and other authorizations)
- Verify any new URL’s (see resource page)



## Resources

<https://bit.ly/cyberstuff>

