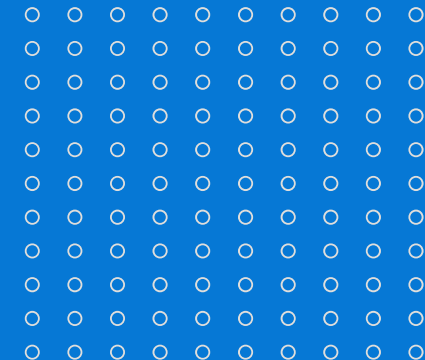
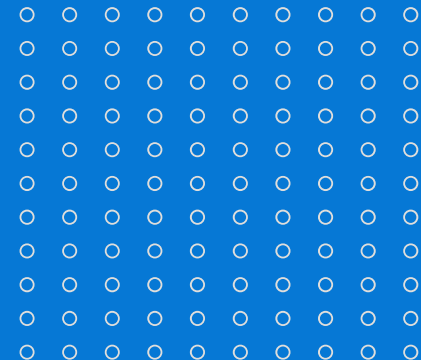
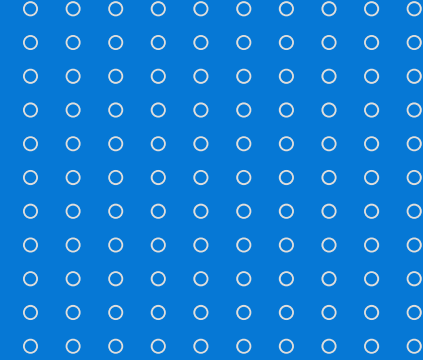


# Cyber Risk: Protecting Your Remote Business

April 16, 2020





## Emily Selck

### **Senior Vice President**

Cyber Liability Practice Leader  
Central and West Regions

### **HUB International**

312-279-4941

emily.selck@hubinternational.com



## Arturo Perez-Reyes

### **Senior Vice President**

Cyber Liability Practice Leader  
California, Nevada, and Utah

### **HUB International**

415-529-3478

arturo.perez-reyes@hubinternational.com



## Benjamin Auton

### **Vice President**

Operations and Security Services

### **SpearTip Cyber Counterintelligence**

800-236-6550

BAuton@spearTip.com

# COVID-19: The Largest Cyber-threat Ever

---

Work from home (WFH) has disrupted standard security

Making possible new perils and threats

Fear and concern makes COVID a lure

Isolation creates many new needs

Attacks coalesce on the opportunities

# In the News

- Phishing with COVID lures is up 667%
- Ecommerce fraud on N95 masks, 400%
- One week if Interpol: 2,000 online links advertising COVID items. Seizure of 34,000 counterfeit masks and “coronavirus medicine”
- Fake cure takedowns of Iron Man and Alex Jones
- Attacks on HC providers and personnel: HHS, IL, etc.
- Payment-fraud campaigns regarding CARE-Act funds
- Chinese military’s APT 41 exploiting the crisis to attack businesses
- US consumers have lost \$5 million to coronavirus scams, according to the FTC
- 80% of all the attacks have something to do with the pandemic, says Proofpoint

## COVID-19 Related Threats in Q1 2020

**907K**

Total spam messages related to COVID-19

**737**

Detected malware related to COVID-19

**48K**

Hits on malicious URLs related to COVID-19

**220K**

Increase in spam from Feb to Mar 2020

**260%**

Increase in malicious URL hits from Feb to March 2020

**United States**

Top location for spam and malware detections, and users accessing malicious URLs

Detection numbers are based on coverage of our Smart Protection Network, which has limited global distribution (collection period January 1 to March 31, 2020)  
Source: Trend Micro | research

# Agenda

- 1 | Are WFH employees and computers covered for cyber protection?
- 2 | What perils can cause disruption or losses?
- 3 | How can firms secure themselves?
- 4 | Questions and answers

# The Post COVID-19 Cyber World

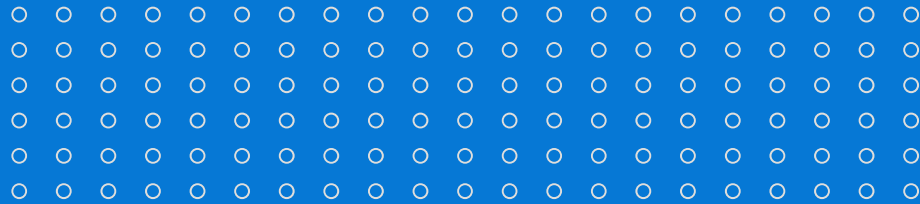
---

The attack surface of networks is completely different

Networks have become completely distributed

Network monitoring and log-based security  
don't protect work from home networks

Endpoint visibility and protection is ideal but  
not everyone has or can afford it



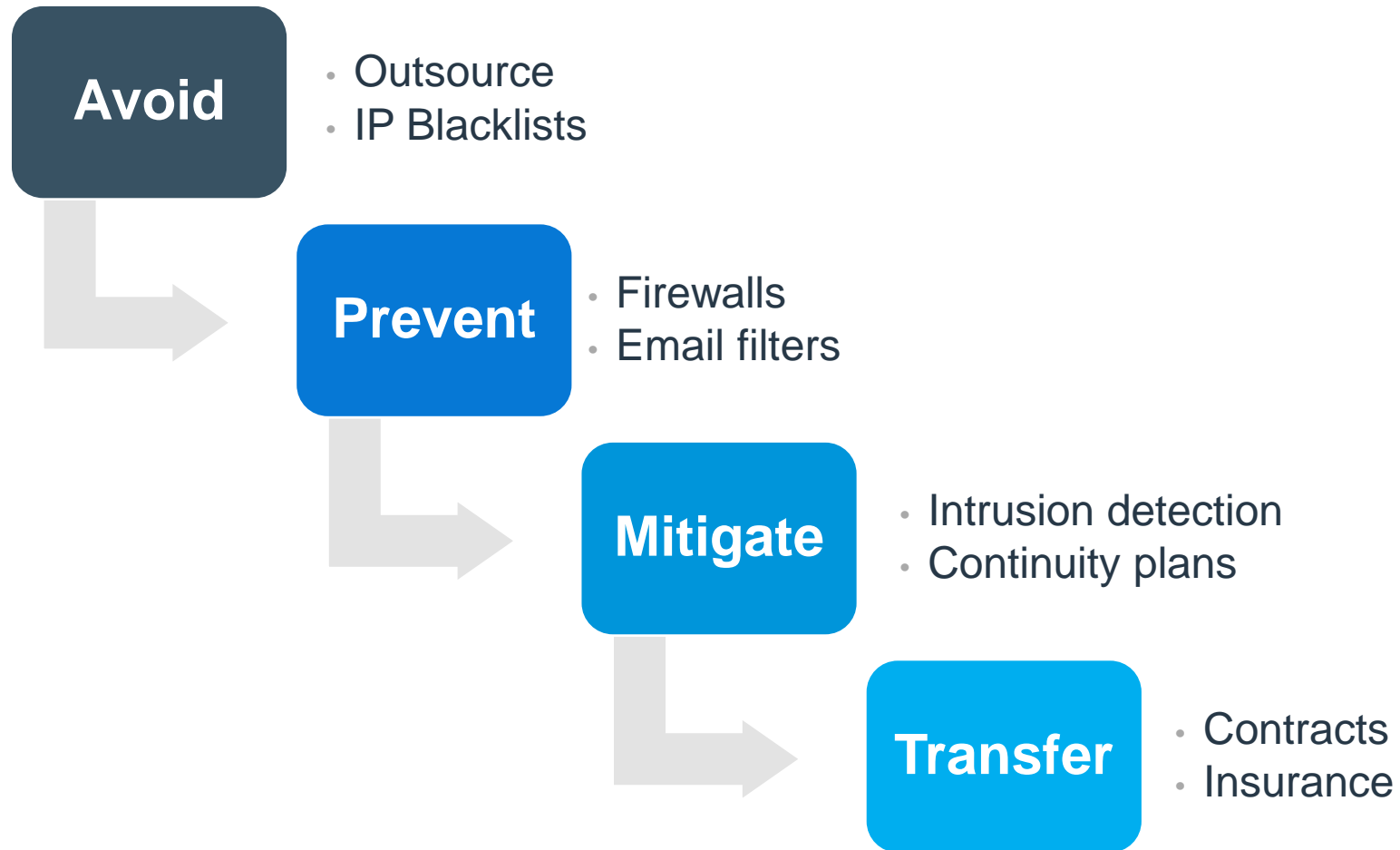
# Risk Management

---





# Risk-solution Stack





# Insurance

## Privacy triggers

- Statutes and laws
- Contracts: NDAs

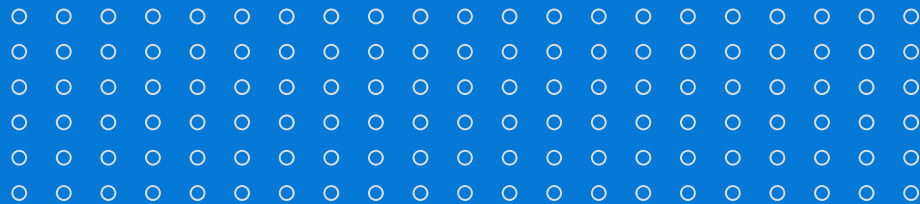
## Security triggers

- Your computers and network
- Your leased cycles and wares
- Your phones and notebooks

## Required Bring Your Own Device (BYOD) policy

### Privacy Breach:

**(a)** the unauthorized collection, disclosure, use, access, destruction or modification of Private Information; **(b)** the inability to access or failure to provide Private Information; **(c)** the theft or loss of Private Information, including the theft or loss of Private Information stored on an unsecured Data storage device or mobile or handheld device, including any smartphone, tablet or laptop which is owned by You and operated by an Insured, or owned and operated by an Employee or Executive who has agreed in writing to Your corporate mobile device acceptable use and security policy (also known as a “Bring Your Own Device” policy);



# Internet Perils

---



# Threat: Phishing

Over the past month, 100,000 new domain names containing COVID, corona, and virus.

**50% are malicious**

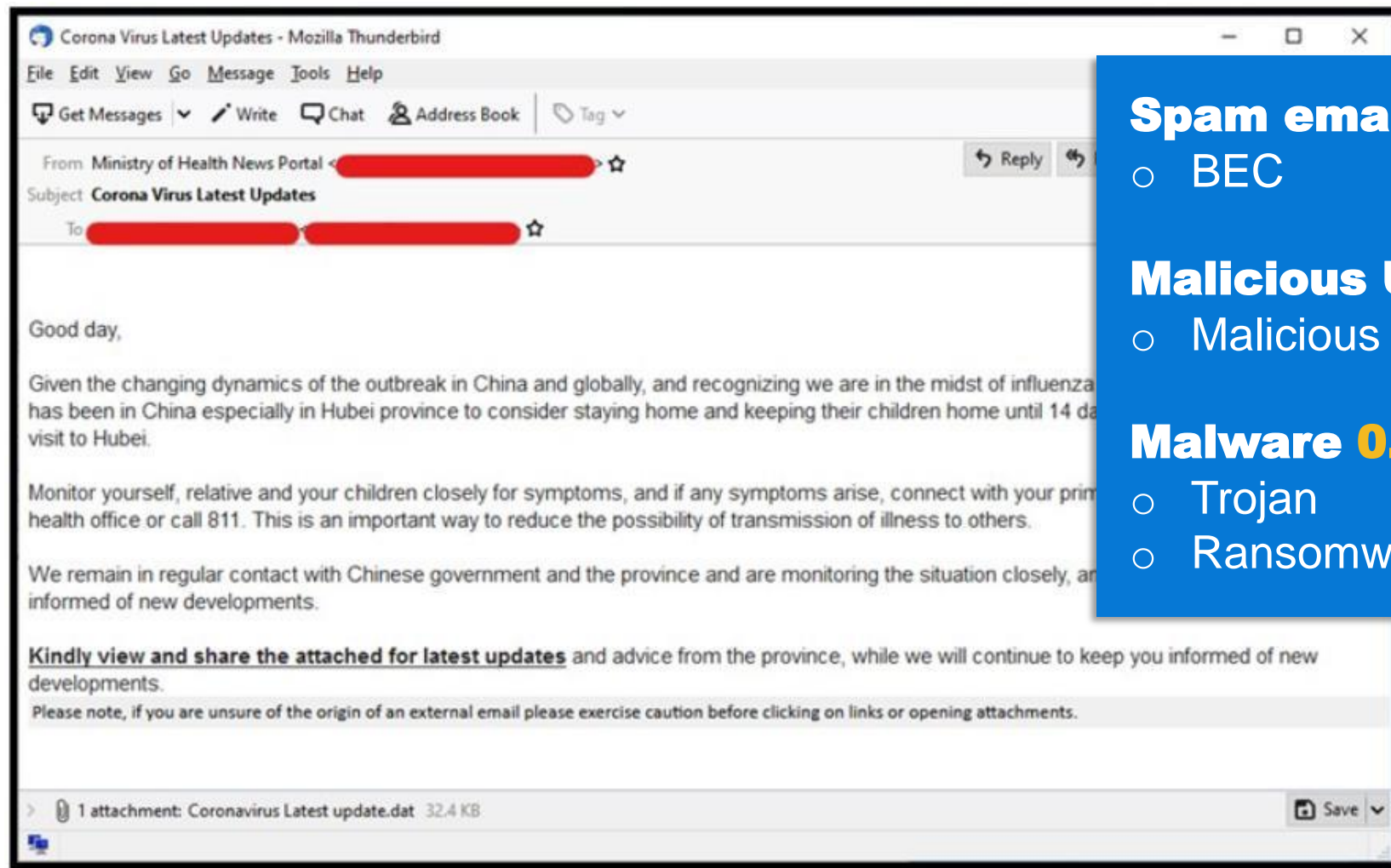
“Spoofed” websites used for phishing credentials **rose by 350%** since January to more than 500,000

## Free tests and training

- Google phish test: <https://phishingquiz.withgoogle.com/>
- Trend Micro: <https://phishinsight.trendmicro.com/en/>
- Media Pro: <https://www.mediapro.com/free-course-stay-secure-work-from-home/>

Sources: ICANN, Atlas VPN

# Threat: Spam



**Spam email 94.9%**

- BEC

**Malicious URLs 5.0%**

- Malicious domains

**Malware 0.1%**

- Trojan
- Ransomware

Sources: TrendMicro

# Ways to Protect Against Email Threats

---

Leverage cloud-based spam filters for email

Mark external email with a warning

Harden the human firewall with training

Stop homograph attacks with AI

# Threat: Websites

The image displays two overlapping web forms. The background form is from the World Health Organization (WHO) and prompts users to verify their account details to download COVID-19 safety measures. It includes a 'COVID-19 SAFETY PORTAL' tab, a 'Login' section with fields for 'Phone Number', 'Email', and 'Password', and a 'Verify' button. The foreground form is from the Centers for Disease Control and Prevention (CDC) and prompts users to sign in with their company email to get on a CDC waitlist. It includes fields for 'Email Address' and 'Password', and a 'Login' button. The CDC form also features a background image of a virus particle.

World Health Organization

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

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

Outlook Gmail Office 365 Yahoo AOL

Sign in with your company email to get on CDC waitlist

Email Address

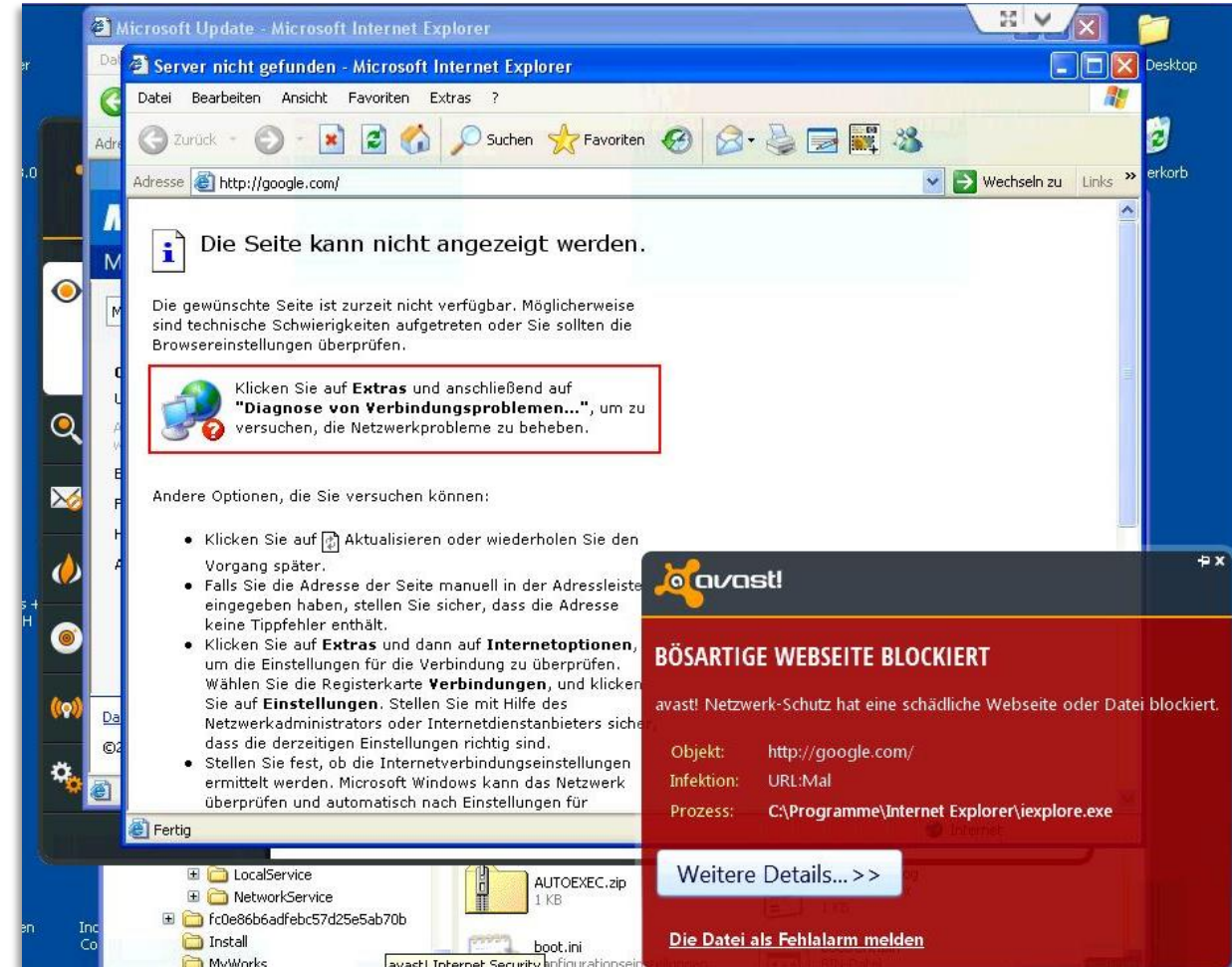
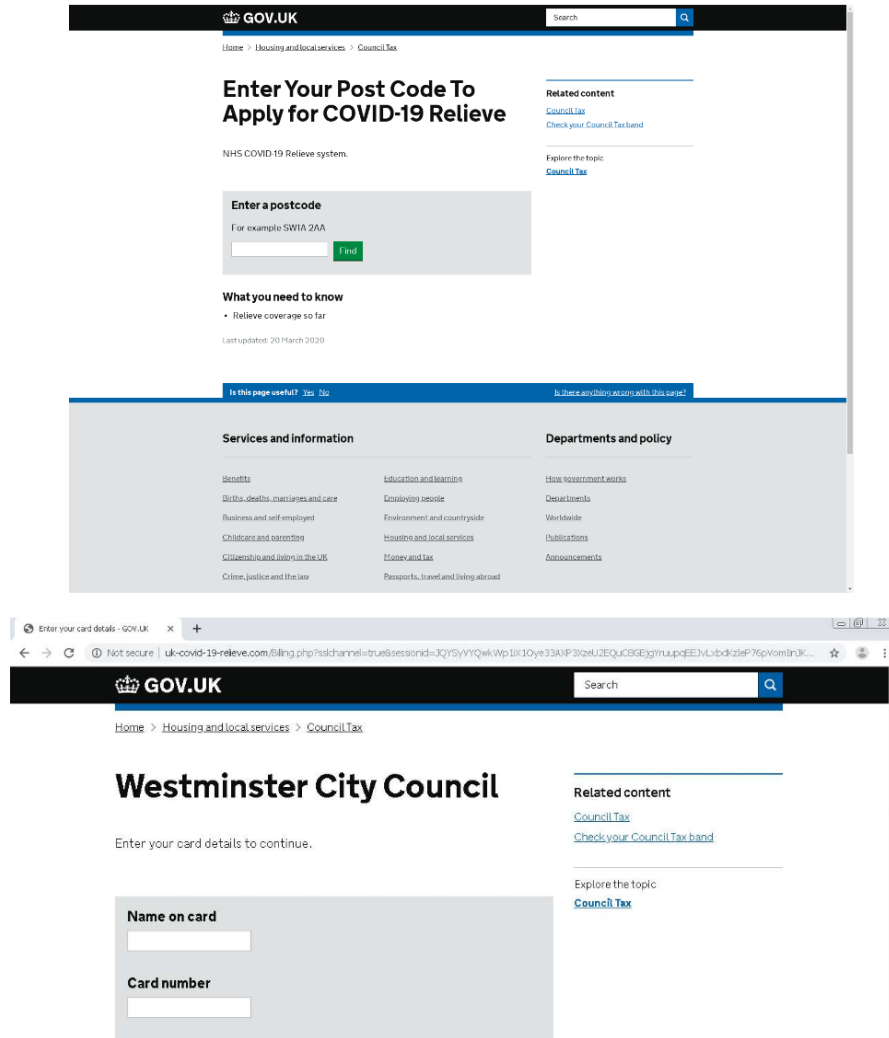
Password

Login

Sources: TrendMicro



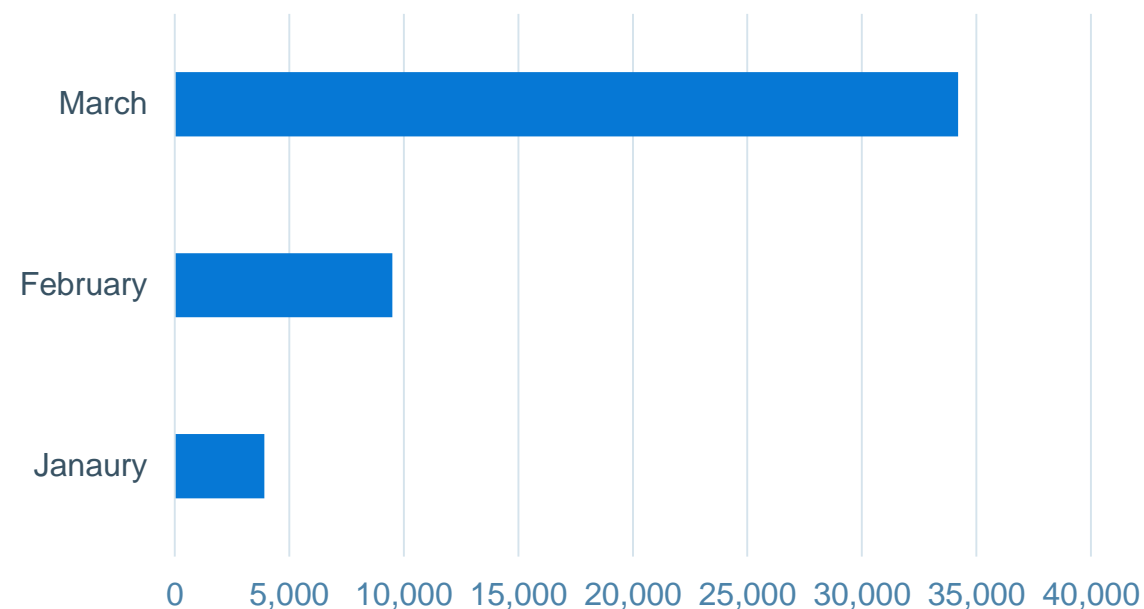
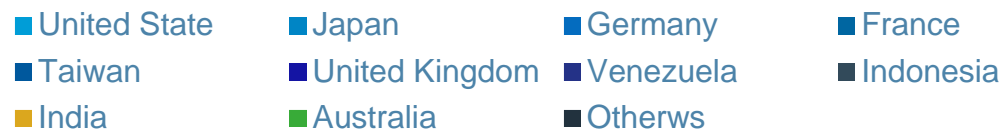
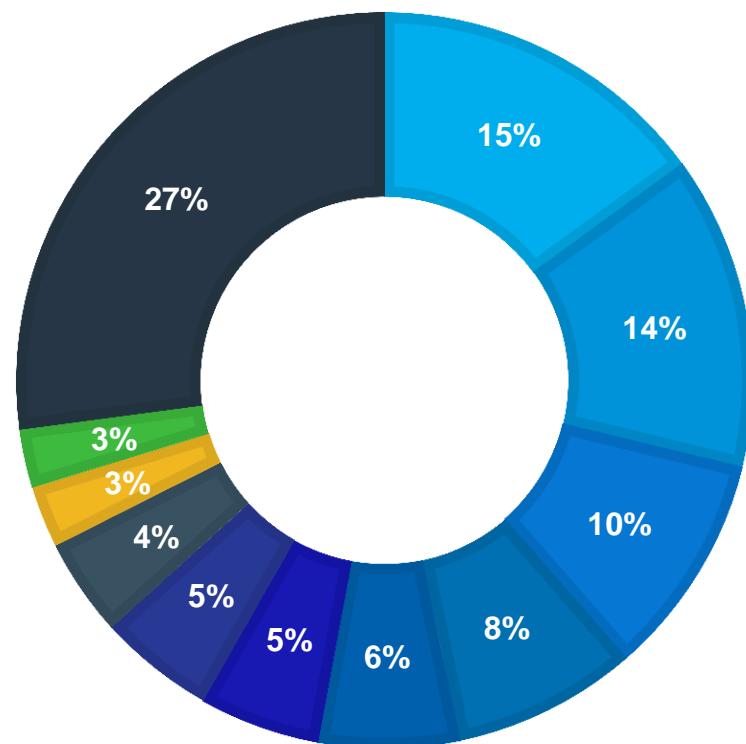
# Threat: Websites



Sources: SuperUser and TrendMicro



# Threat: Domain names



Sources: TrendMicro

# Ways to Protect Against Website Threats

---

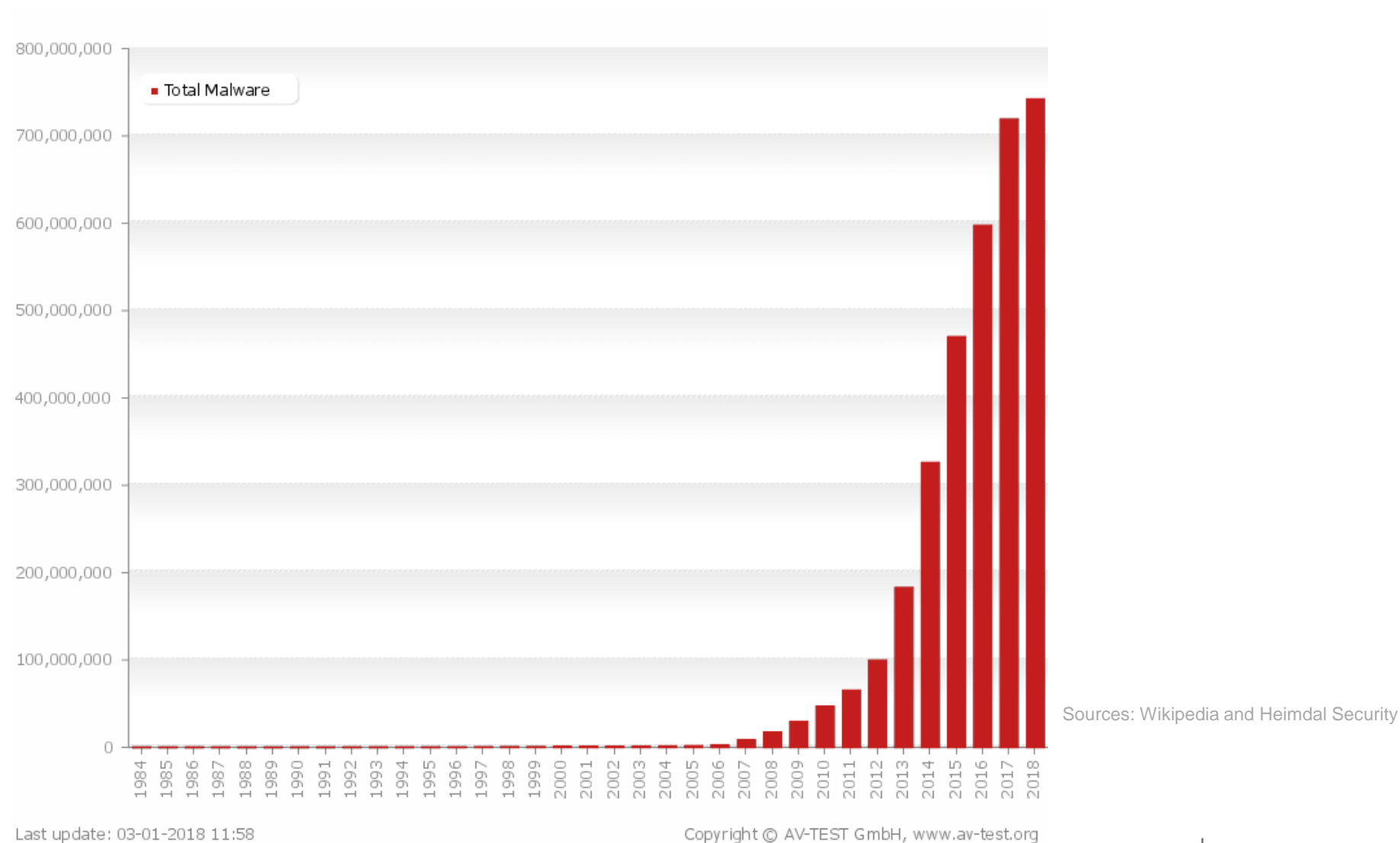
Filter network to block harmful websites or needless nations

Users should avoid embedded links. Go directly or via search

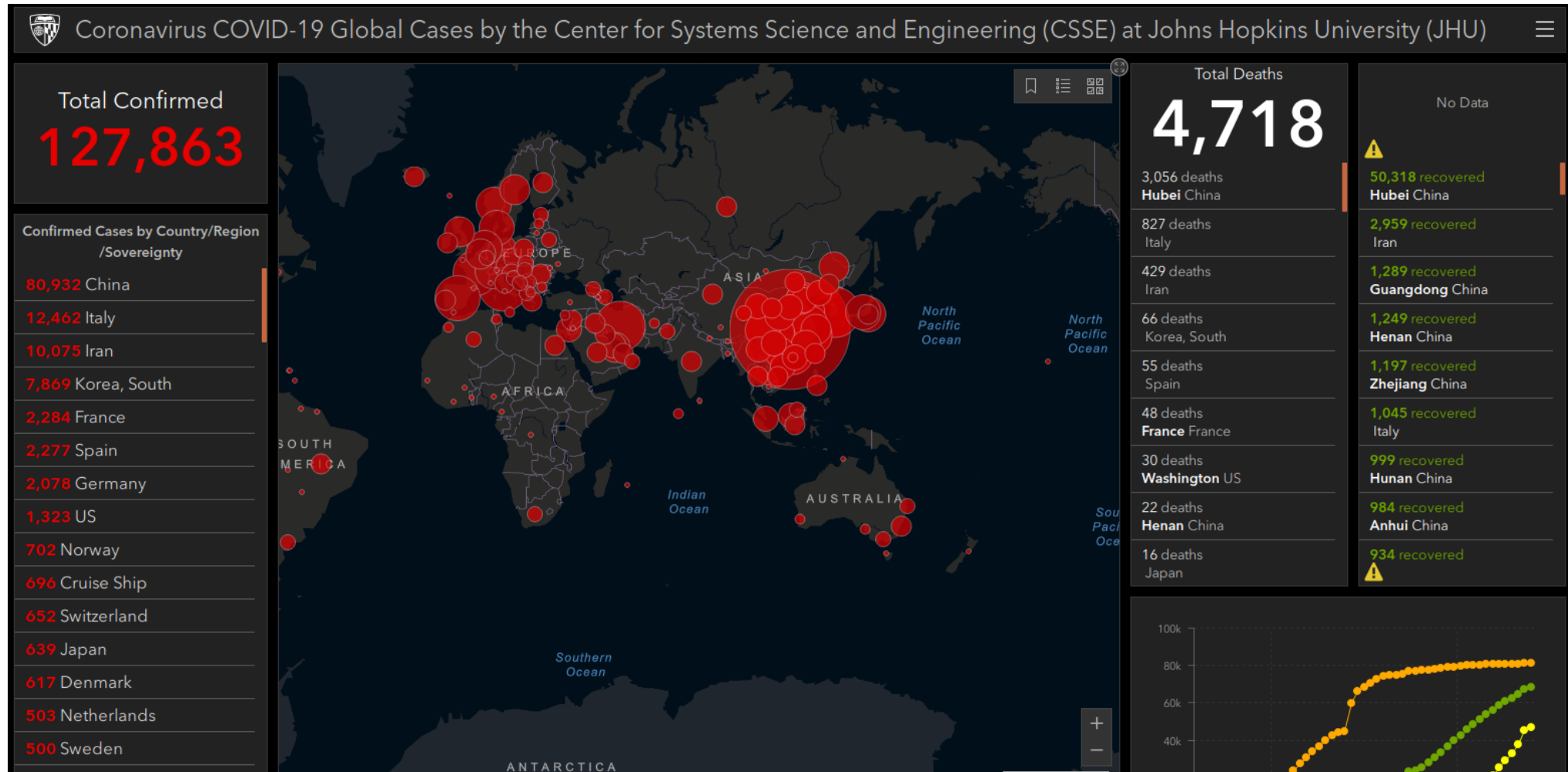
Provide links to legitimate COVID-19 resources

Warn users about fake websites and campaigns

# Threat: Malware



# Threat: Malware



# Threat: Ransomware

**YOUR PC IS LOCKED**

If you want to unlock your files you must send 0.35 BTC (Bitcoin) to the

1wNyr6A5ZCUxE2fShTvUGPtHfuovT7uBt

After payment send email to : RASOM20@secmail.pro  
Insert in message : transaction id - Pc Name - Username

temporarily blocked on several levels.  
military secret encryption algorithm.

Encrypting your files, you must do the following:  
to Bitcoin wallet bclq6ryyex33jxgr946u3jyr  
receipt Bitcoin;  
e-mail: coronaVi2022@protonmail.ch and tel

to Bitcoin transaction generated or Bitco  
you get in your email the following:  
and software to unlock your computer  
cryptor of your files.  
US presidential elections are accepted aro  
i hic intras! [Wait to payment timeout 25

Sources: ThreatPost and ThreatFix

# Ways to Protect Against Computer Viruses

Use a 3-2-1 backup strategy and use it regularly

Keep all computers and software up to date and use anti-virus software

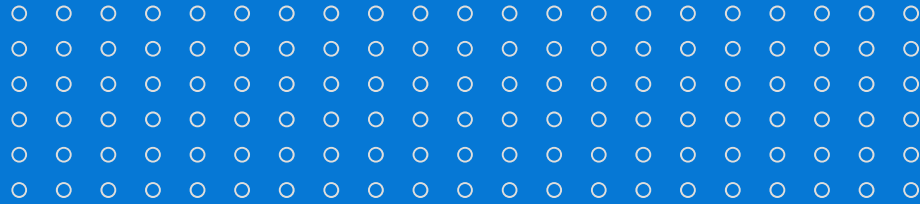
Remove local administrator privileges on company-owned devices

At home, never work or browse as a sysadmin. Use two accounts

Remote Desktop Protocol is not a VPN. Do not access a corporate network.  
If you need remote access use a secure solution

Managed Detection and Response (MDR) is effective against malware and ransomware. It combines tools to monitor computers with IT security experts that respond to malicious activity





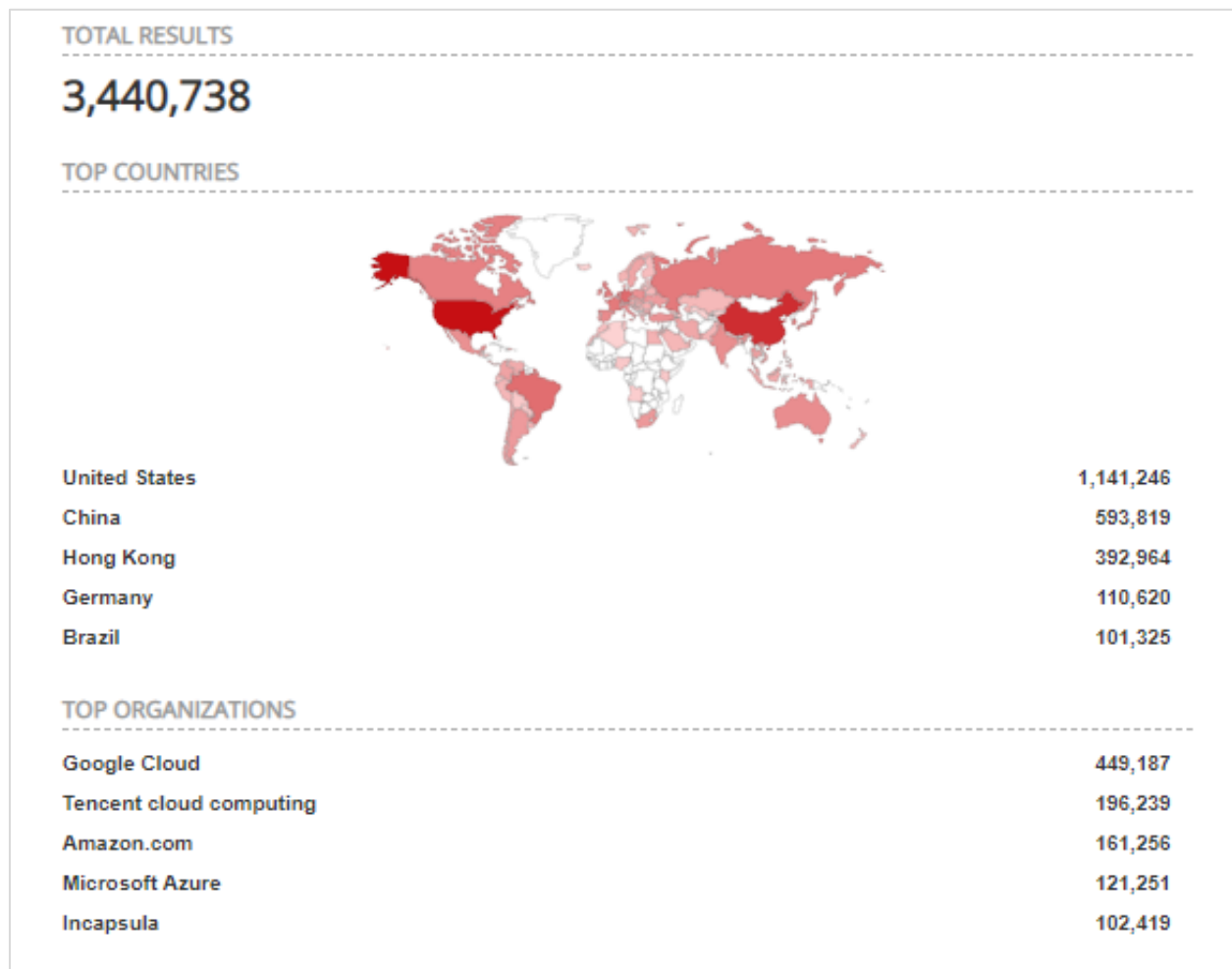
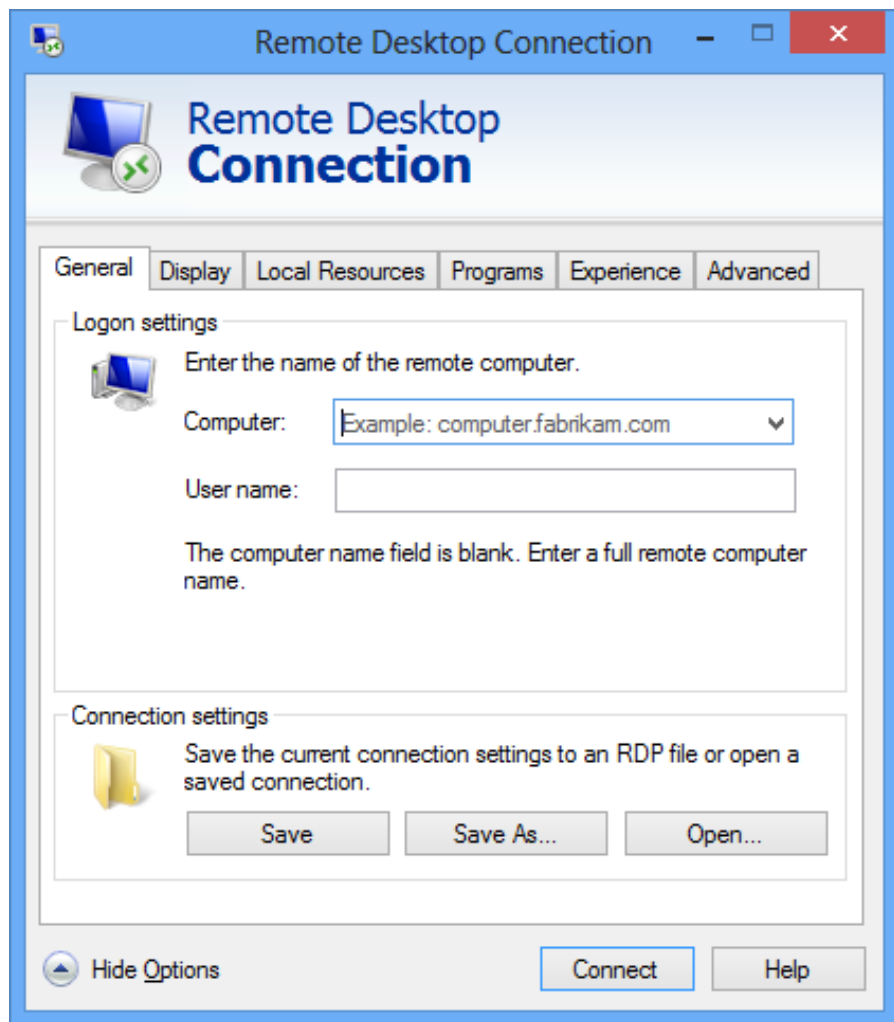
# Platform Perils

---






# Threat: Remote Desktop Connections



Sources: Microsoft and Avast

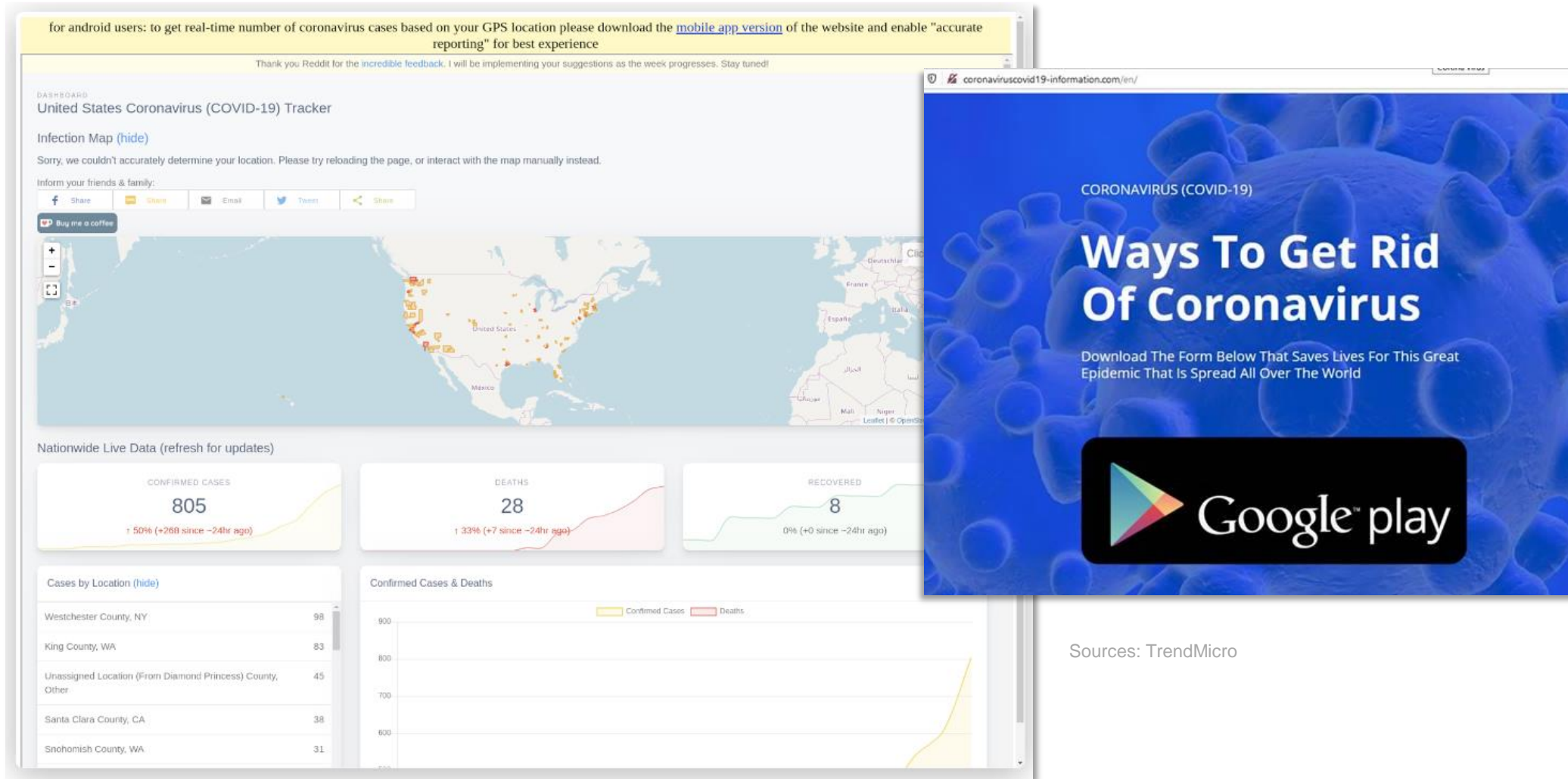
# Threat: Applications



**Microsoft Office Word 2020 restored:**  
This document was created in last version of Word Application  
To view full content please, click "**Enable Editing**", "**Enable Content**"

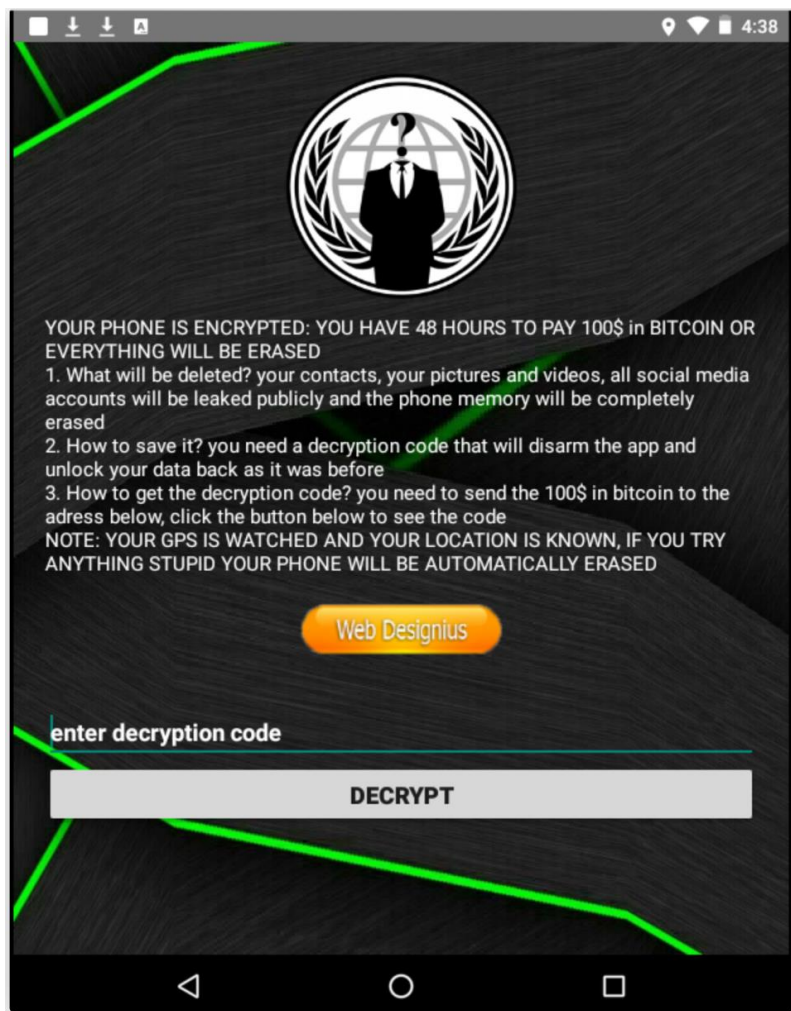
3076	3/08/2013 10:14 PM	File folder	
3082	3/08/2013 10:14 PM	File folder	
Graphics	3/08/2013 10:14 PM	File folder	
Setup	14/05/2013 8:58 PM	Application	78 KB
SetupUtility	14/05/2013 8:53 PM	Application	98 KB
SetupEngine.dll	14/05/2013 8:59 PM	Application extens...	792 KB
SetupUi.dll	14/05/2013 8:58 PM	Application extens...	290 KB
sqmapi.dll	14/05/2013 8:53 PM	Application extens...	192 KB
header	14/05/2013 9:26 PM	BMP File	4 KB

# Threat: Mobile

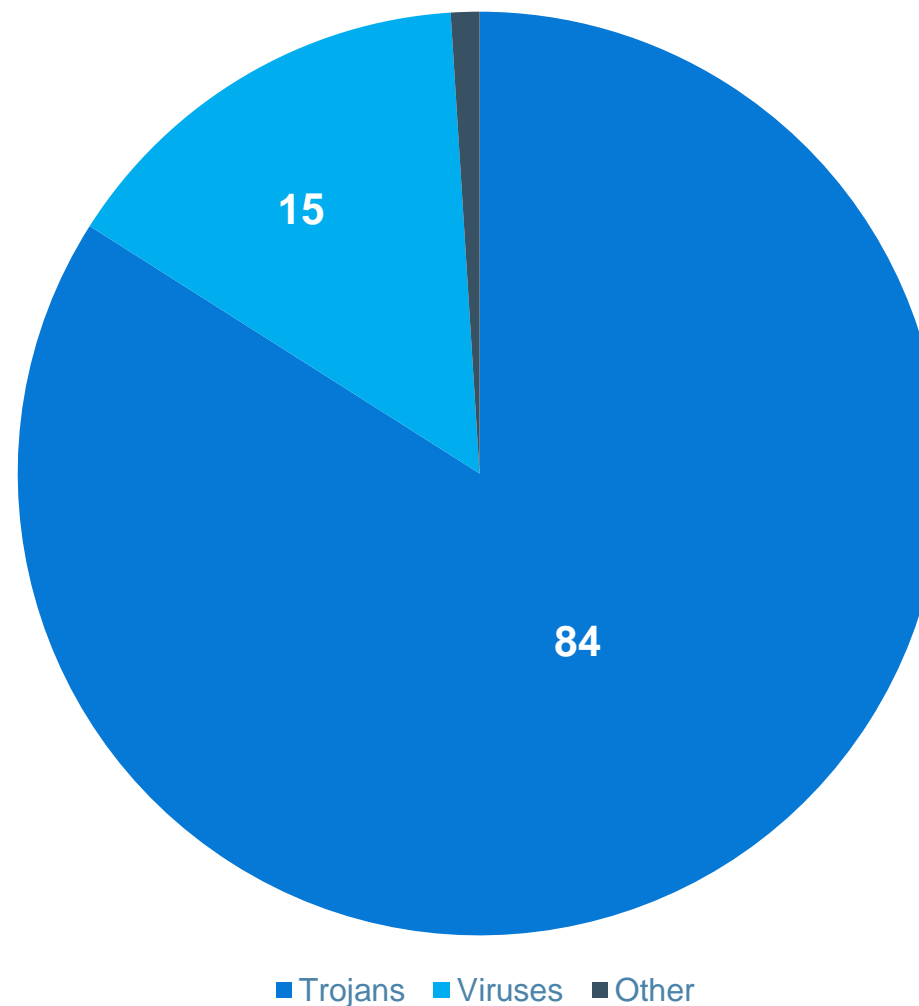


Sources: TrendMicro

# Threat: Mobile



Sources: Wikipedia and TrendMicro



# Threat: Conferencing

---

**Bombing**

**War Dialing**

**Encryption**

**Routing**

**Tracking**

**Vulnerabilities**

Sources: Various

# Ways to Protect Against Various Platform Threats

---

Educate users on where to download legitimate apps

Users should only use the Google Play and iOS app store

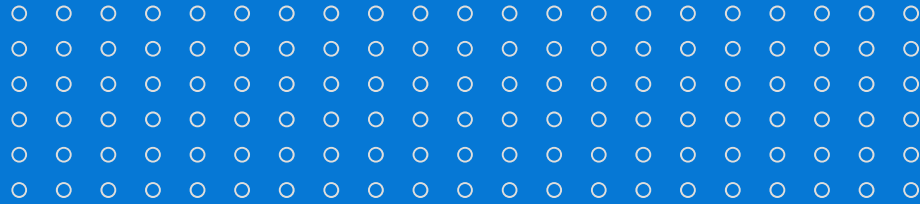
Make sure your Android device has a passcode

Do not allow children to use mobiles unsupervised

Consider using a mobile-device manager

Never jail break a phone





# Content Perils

---





# Threat: Extortion

From: [REDACTED]

Date: March 26, 2020 at 1:06:42 PM GMT+8

To: "[REDACTED]" >

Subject: I can infect you with COVID-19

I know everything little secret about your life.

To prove my point, that is why i am sending you this email from your system using your email account.

I am aware of your whereabouts, what you eat, with whom you talk to, every little thing you do everyday.

**What am i capable of doing?**

If i want, i could infect You and your whole family with the Corona Virus (COVID-19).

Reveal all your secretes, There are countless things i can do.

**What should you do?**

transfer the amount of \$500 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin" or <https://www.coinmama.com>).

**My bitcoin address (BTC Wallet) is: 1HEGxH9pZwYCnxf2PQCvyKzB2JzairA82W**

After receiving the payment, you will never hear me again.

**I give you 72 hours (NOT more than 3 days) to pay**, failure to do this, I will infect YOU and every member of your family with the Corona Virus (COVID-19).

no matter how smart you are, and believe me, i will completely ruin your life.

I have a notification reading this letter, and the timer will start to work when you see this letter.


Don't waste your time replying this email because it was sent from your system and email account.

**If I find out that you have shared this message with someone else or try to report this, Then YOU and every member of your family will be infected with the Corona Virus (COVID-19).**

# Threat: Fraud

Coronavirus Masks N95 Authentic 3M Respirators

03-09-2020, 05:35 PM



125

16

4 0 0

187.5

0


I have authentic 3m N95 Masks for sale.

These are for the COVID-19 Virus spreading internationally. This virus will continue to spread as there is no cure for now and the only way to protect yourself in public is to wear protection. Confirmed cases in New York went from 45 to 150 in the past 48 hours.

Looking to sell these for \$15 each individually including shipping. Paypal or BTC

If you want to buy in bulk or resell PM me for pricing, serious discounts.

Have 1,350 in stock in USA.



Start Contract

PREMIUM TOILET PAPER | MADE IN GERMANY | 3&4 layer ones available!!!!

Posted 17 March 2020 : 08:17 AM

PREMIUM TOILET PAPER MADE IN GERMANY

Everyone knows that made in Germany stands for quality.

I have two kinds of toilet paper:

3 layers

4 layers

both come without any aroma

Price per roll:

3 layer one: 12€

4 layer one: 15€

Shipping in Germany: free

Every other country: you have to cover the shipping fees



My ass can vouch for the quality

Payment options: PayPal, BitCoin

Sources: TrendMicro

31

© 2020 HUB International Limited.

# Threat: Misinformation Campaigns

---

**Bioweapon Blame**

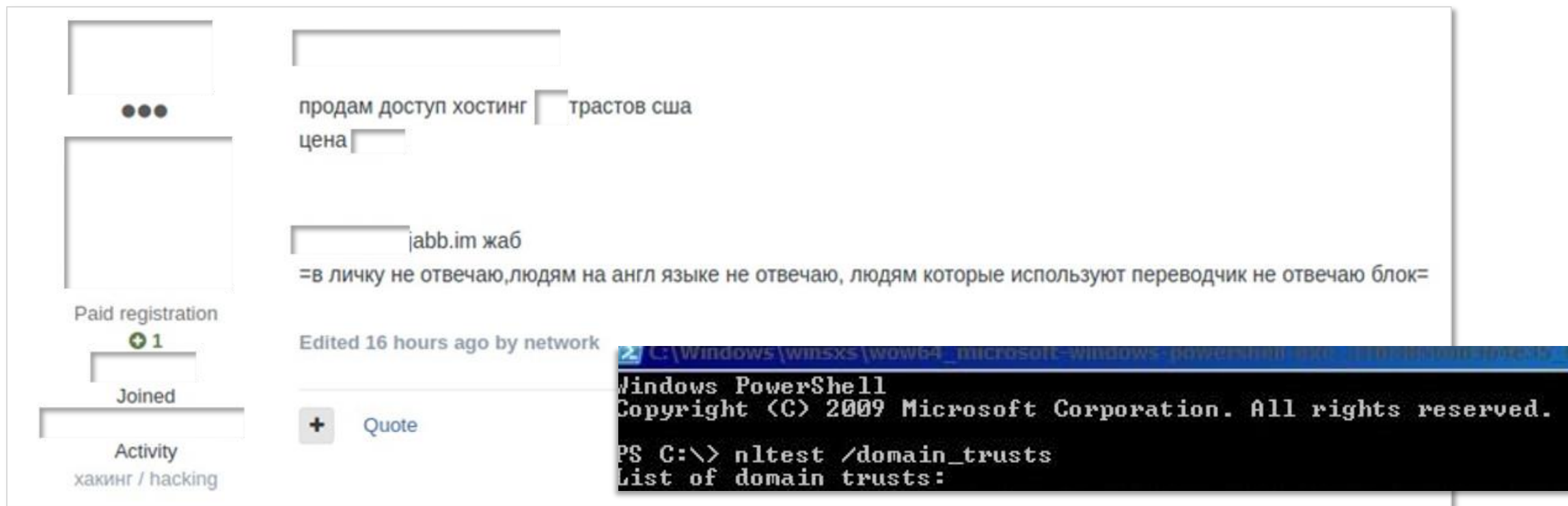
**5G Cell Towers**

**Quinine**

**Caffeine**

Sources: Various

# Case Study: Selling Access to Your Network



## Approximate Translation

“I don’t answer in PM, I don’t answer people in English, I don’t answer the block for people who use the translator”

# Ways to Protect Against Personal Threats

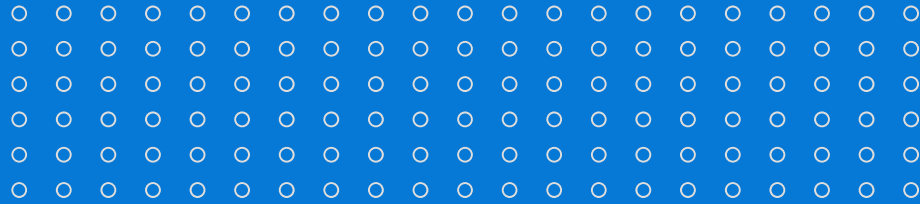
Never re-use passwords. Use a password manager to remember long and complex passwords or phrases

Avoid watering-hole websites that infect with malware: gaming, porno, MP3 rippers, free software, free anything for that matter

Harden the web browsers so that they are not so easily hijacked by javascript and consider a filtering plug-in that kills bad sites

Look out for the six P's of fraudsters:  
1) Place, 2) Prescriptions, 3) Promises, 4) Price, 5) Privacy, 6) Product

Double check inflammatory or “miraculous” content with experts or fact checkers. Remember: big claims require bigger evidence



# Securing the Home Office

---



# How Businesses Can Secure Data

---

## **User Awareness**

- No longer focused on just phishing emails
- Educate your users on best practices

## **Change Control**

## **Strong Credentials with Multifactor**

## **Incident Identification Considerations**

## **IT Support for Personal Devices**

## **Endpoint Visibility**



# Business Data Security Checklist

---

- ❑ Passwords are weak. Use multi-factor authentication
- ❑ Issue preconfigured company laptops and mobiles
- ❑ Equip equipment with a security suite of tools
- ❑ Back-up data using the 3-2-1 rule: three copies in two with one off-site
- ❑ Limit VPN access and force renewed logins periodically
- ❑ Enhance monitoring for detection of abnormal activity
- ❑ Train and test your workforce on privacy, phishing, and social engineering
- ❑ Don't rely on people. Filter mail. Harden endpoints

# Business Data Security Checklist

---

- ❑ Educate employees on coronavirus scams
- ❑ Make it easy for workers to check or report problems and get assistance
- ❑ Crisis and IR plans need to be executable by a remote workforce
- ❑ Use remote collaboration, conference bridges, and messaging tools so a dispersed team can work and respond to problems

# Employee Data Security Checklist

---

- ❑ Use company equipment; avoid home machines
- ❑ If using own machines, update and patch wares. Make close as possible to office standards
- ❑ Use company security wares, follow data protection policies, avoid personal browsing on sensitive machines
- ❑ Avoid free, public Wi-Fi. Use enterprise VPN servers to connect to work networks
- ❑ Where secure connectivity is doubtful, use encrypted email or encrypted file storage sites
- ❑ Change the admin passwords on your WiFi router. Turn on WPA encryption. Split the network to isolate yourself; e.g. guest net or VLAN

# Employee Data Security Checklist

---

- ❑ Create two user accounts: only use the super-user account for installs; work from a personal account with limited privileges
- ❑ Never reuse a password. Use a password manager to generate and store long and unique passwords
- ❑ Online bank from a dedicate machine or a Linux distro
- ❑ Have a personal backup solution that uses 3-2-1
- ❑ Routinely scan your network to identify all connected devices
- ❑ Routinely scan your computers for malware and adware
- ❑ Lock down the browser against javascript and malicious IP addresses
- ❑ Be wary of scams

# Revise Company Data & Device Policies

## **BYOD Policy for Insurance**

VPNs | Storage | Devices

## **Work From Home Policy**

Hours | Acceptable Use | Devices | Security

Business Continuity and Disaster Recovery Plans

Incidence-response and Crisis Plans  
Done remotely?

Insurance Requires Two Phone Calls  
Claims and Coach

# Resources

---

- 1) [COVID-19 Security Resource Library](#)
- 2) [Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions](#)
- 3) [SANS Security Awareness Guide – Securely Working at Home](#)
- 4) [CISA guidance for defending against COVID-19 cyber scams](#)
- 5) [NCSC dealing with suspicious emails and messages](#)
- 6) [NCSC guidance on home working](#)
- 7) [IAPP BYOD Policy Template](#)





**Be prepared.  
Know how to respond.**

Visit HUB's Coronavirus Resource Center at  
**[hubinternational.com](https://hubinternational.com)**

# Thank you.

