UNIVERSITY of HAWAI'I®
MAUI COLLEGE

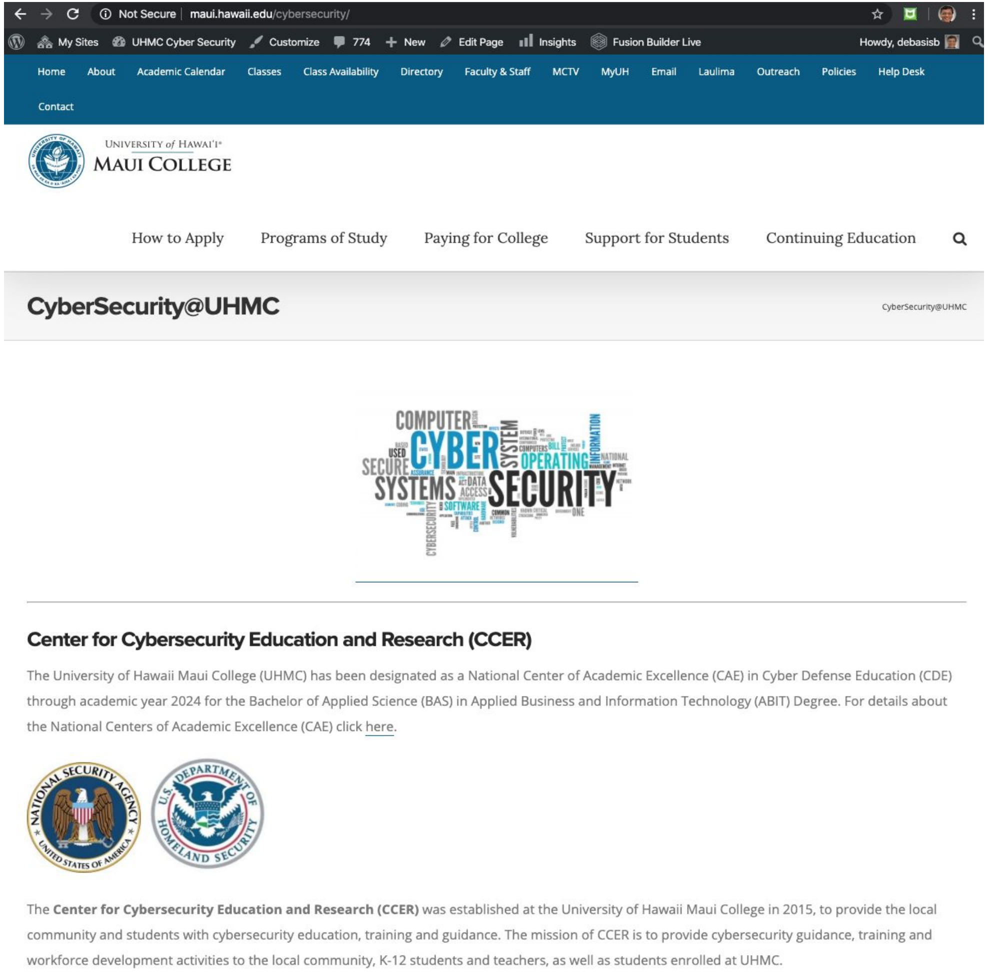
Cybersecurity Trends & Defenses: What You Can Do About It!

Debasis Bhattacharya (debasisb@hawaii.edu)
Jonathan Chee (Jonathan.Chee@k12.hi.us)

Presentation available @ maui.hawaii.edu/cybersecurity
July 23, 2020

Agenda

- Introductions - 10 minutes
  - Debasis Bhattacharya, Brook Conner, Jonathan Chee
- Working from Home - Security Guidance -
  - Monitor Changing Threat Landscape - 10 minutes
  - Secure Your Home Office - 15 minutes
  - Secure Your Home Environment - 15 minutes
  - Secure Your Virtual Meetings - 10 minutes
- Hi DoE Security Guidance - 30 minutes
- Q&A - 30 minutes



CyberSecurity@UHMC

Center for Cybersecurity Education and Research (CCER)

The University of Hawaii Maui College (UHMC) has been designated as a National Center of Academic Excellence (CAE) in Cyber Defense Education (CDE) through academic year 2024 for the Bachelor of Applied Science (BAS) in Applied Business and Information Technology (ABIT) Degree. For details about the National Centers of Academic Excellence (CAE) click here.

The **Center for Cybersecurity Education and Research (CCER)** was established at the University of Hawaii Maui College in 2015, to provide the local community and students with cybersecurity education, training and guidance. The mission of CCER is to provide cybersecurity guidance, training and workforce development activities to the local community, K-12 students and teachers, as well as students enrolled at UHMC.

Source: http://maui.hawaii.edu/cybersecurity/

Debasis Bhattacharya

Dr. Debasis Bhattacharya (Debāśiṣ Bhaṭṭāchārya, দেবাশীষ ভট্টাচার্য, देवाशीष भट्टाचार्य) is currently a tenured faculty member at the University of Hawai'i Maui College, and program coordinator for the Applied Business and Information Technology (ABIT) baccalaureate program. Dr. Bhattacharya has been working in the software and higher education industry for 32 years, having worked for large corporations such as Oracle and Microsoft for 15 years.

A resident of Hawaii since 2002, he has been actively researching the information security needs of small businesses since 2008. As a former small business owner, he understands the needs and demands of information security, as well as keeping a small business up and running! Dr. Bhattacharya holds degrees from MIT, Columbia University, University of Phoenix and NW California University School of Law. Research interests include computer science education, cybersecurity, cryptocurrencies, blockchains and machine learning.

Jonathan Chee

Ofc of Info Tech Svcs

Information Security Manager

Enterprise Architecture Branch

Currently Acting Chief Information Security Officer for the Department of Education. Has 16 years of information security experience. Prior to joining the DOE he worked at various banks and credit unions which I was responsible for all aspects of security and the planning and integration of end-to-end security solutions.

David Brookshire "Brook" Conner, Assistant Superintendent & Chief Information Officer,
Office of Information Technology Services

David Brookshire "Brook" Conner was appointed on Sept. 25, 2017 to oversee HIDOE’s information and telecommunication systems, facilities, and services of the public school system and department-wide operations. The Office of Information Technology Services (OITS) ensures that information technology and telecommunications support are being provided efficiently and effectively, and in accordance with laws, policies, and accepted principles of management. The scope of OITS’ technical oversight includes voice, data, video, information systems infrastructure, and support services for schools and for complex areas and state administrative offices. Support services to schools are exercised in collaboration with the complex area superintendent.

Conner has served in high-profile information technology (IT) positions, most recently as the first chief information security officer and vice president for Estée Lauder Companies where he constructed a cyber security program, managed a budget of $22 million and ensured compliance. He also worked for Morgan Stanley as an executive director and global head of vulnerability management, Bloomberg LP, and as an adjunct professor at New York University. Conner has also published numerous books and papers on a variety of IT topics.

Jodi Ito

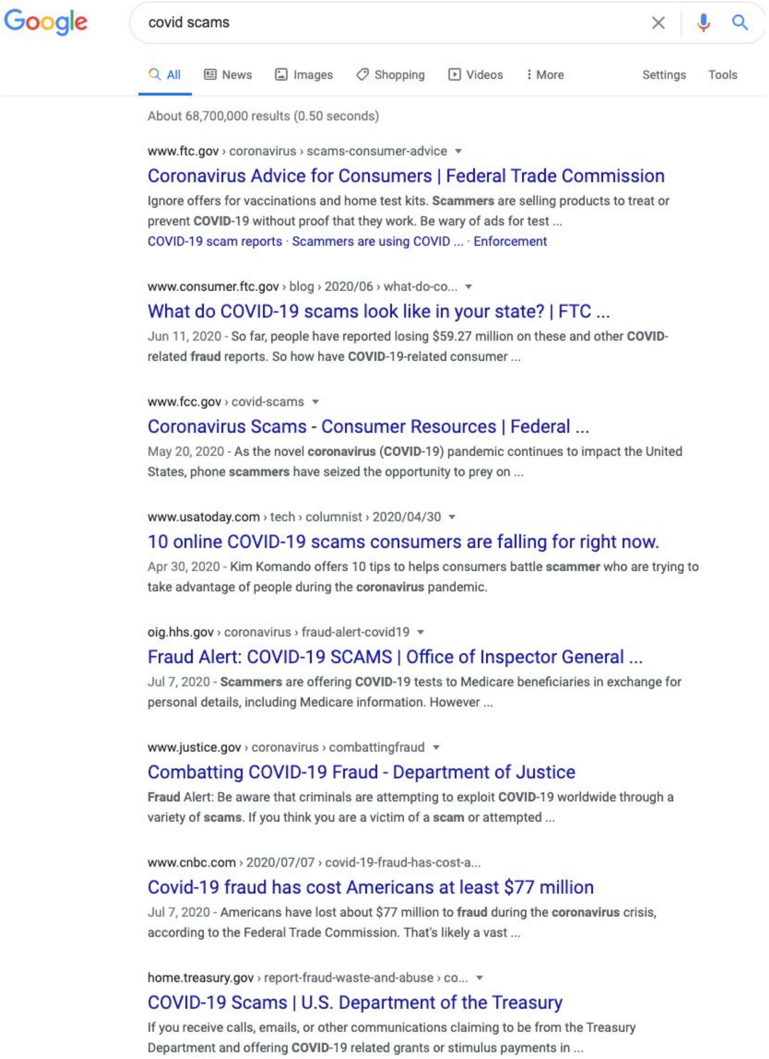
Jodi Ito is the Chief Information Security Officer with the University of Hawaii (UH) System in the Office of the Vice President for Information Technology since 2000 and has been with the University since 1982.

She is responsible for the security and protection of the information assets across the University of Hawaii System. These responsibilities include the development and management of policies and procedures for the UH information security program, conducts risk & vulnerability analysis for critical assets, oversees investigations into cyber incidents, & develops/conducts training on information policy & security issues across all 10 UH campuses and affiliated research & education centers. She has also organized several large scale red/blue team cybersecurity exercises on the UH cyber range involving University students, Hawaii National Guard, military, state and federal government agencies. Jodi graduated with both BS and MS degrees in Computer Sciences from UH Manoa.

Monitor Changing Threat Landscape

Emergence of all sorts of new factors - great opportunity for global cyber hackers!

- Covid-19
  - Hacks using spam, keywords, fake websites, malware, ransomware, extortion etc
  - WHO, CDC, Johns Hopkins Virus Map, N95 masks, Ventilators etc.
- Working from home
  - Hacks including weak router passwords
  - Risks to children confined to home
- Virtual meetings
  - Hacks on Zoom
- Census 2020
- Global Economic Disruption
  - Stimulus checks, unemployment, recession etc.



covid scams

About 68,700,000 results (0.50 seconds)

www.ftc.gov › coronavirus › scams-consumer-advice

Coronavirus Advice for Consumers | Federal Trade Commission

Ignore offers for vaccinations and home test kits. **Scammers** are selling products to treat or prevent **COVID**-19 without proof that they work. Be wary of ads for test ...

COVID-19 scam reports · Scammers are using COVID ... · Enforcement

www.consumer.ftc.gov › blog › 2020/06 › what-do-co...

What do COVID-19 scams look like in your state? | FTC ...

Jun 11, 2020 - So far, people have reported losing $59.27 million on these and other **COVID**-related **fraud** reports. So how have **COVID**-19-related consumer ...

www.fcc.gov › covid-scams

Coronavirus Scams - Consumer Resources | Federal ...

May 20, 2020 - As the novel **coronavirus** (**COVID**-19) pandemic continues to impact the United States, phone **scammers** have seized the opportunity to prey on ...

www.usatoday.com › tech › columnist › 2020/04/30

10 online COVID-19 scams consumers are falling for right now.

Apr 30, 2020 - Kim Komando offers 10 tips to helps consumers battle **scammer** who are trying to take advantage of people during the **coronavirus** pandemic.

oig.hhs.gov › coronavirus › fraud-alert-covid19

Fraud Alert: COVID-19 SCAMS | Office of Inspector General ...

Jul 7, 2020 - **Scammers** are offering **COVID**-19 tests to Medicare beneficiaries in exchange for personal details, including Medicare information. However ...

www.justice.gov › coronavirus › combattingfraud

Combatting COVID-19 Fraud - Department of Justice

Fraud Alert: Be aware that criminals are attempting to exploit **COVID**-19 worldwide through a variety of **scams**. If you think you are a victim of a **scam** or attempted ...

www.cnbc.com › 2020/07/07 › covid-19-fraud-has-cost-a...

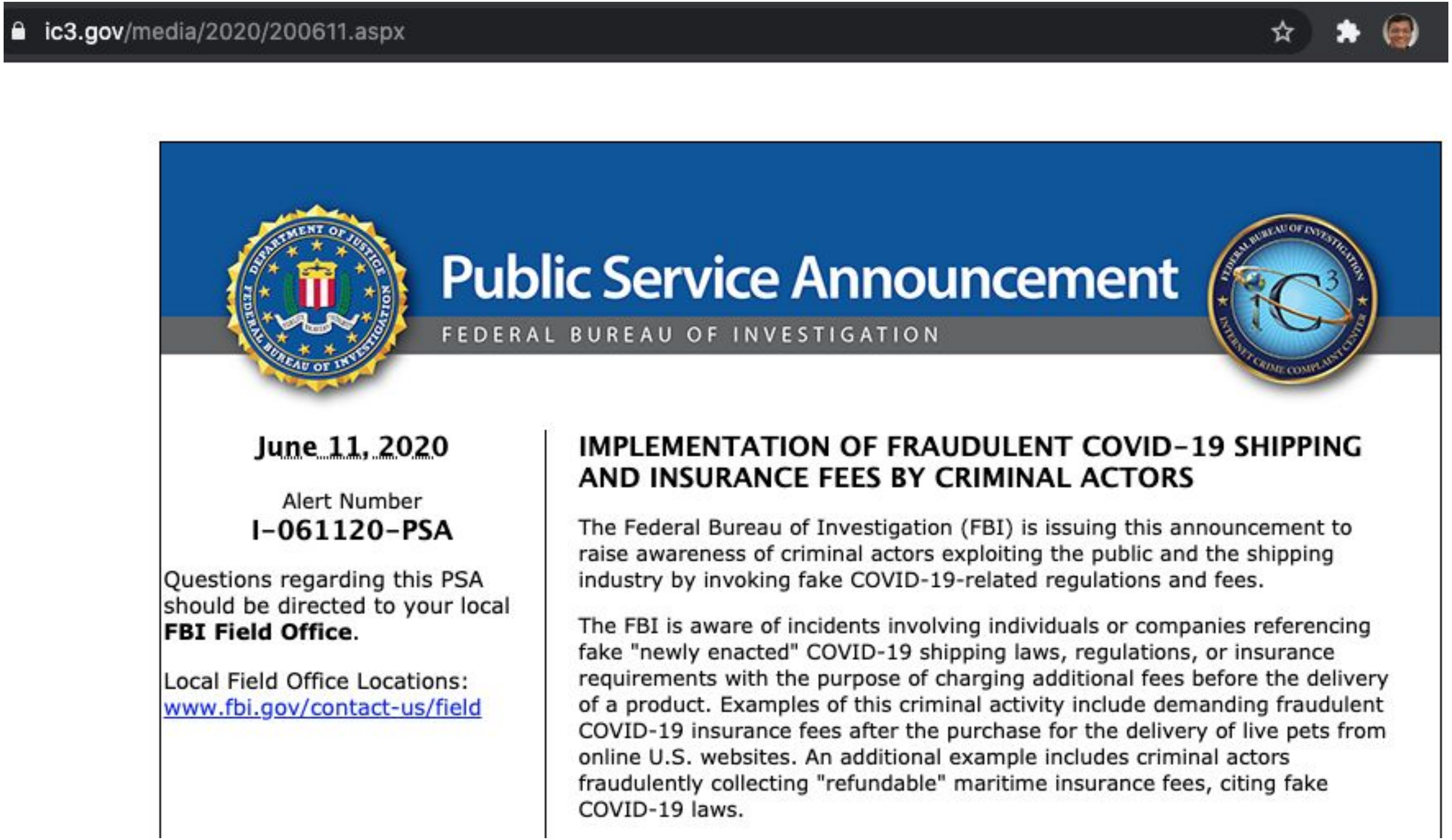
Covid-19 fraud has cost Americans at least $77 million

Jul 7, 2020 - Americans have lost about $77 million to **fraud** during the **coronavirus** crisis, according to the Federal Trade Commission. That's likely a vast ...

home.treasury.gov › report-fraud-waste-and-abuse › co...

COVID-19 Scams | U.S. Department of the Treasury

If you receive calls, emails, or other communications claiming to be from the Treasury Department and offering **COVID**-19 related grants or stimulus payments in ...



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 11, 2020

Alert Number

I-061120-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

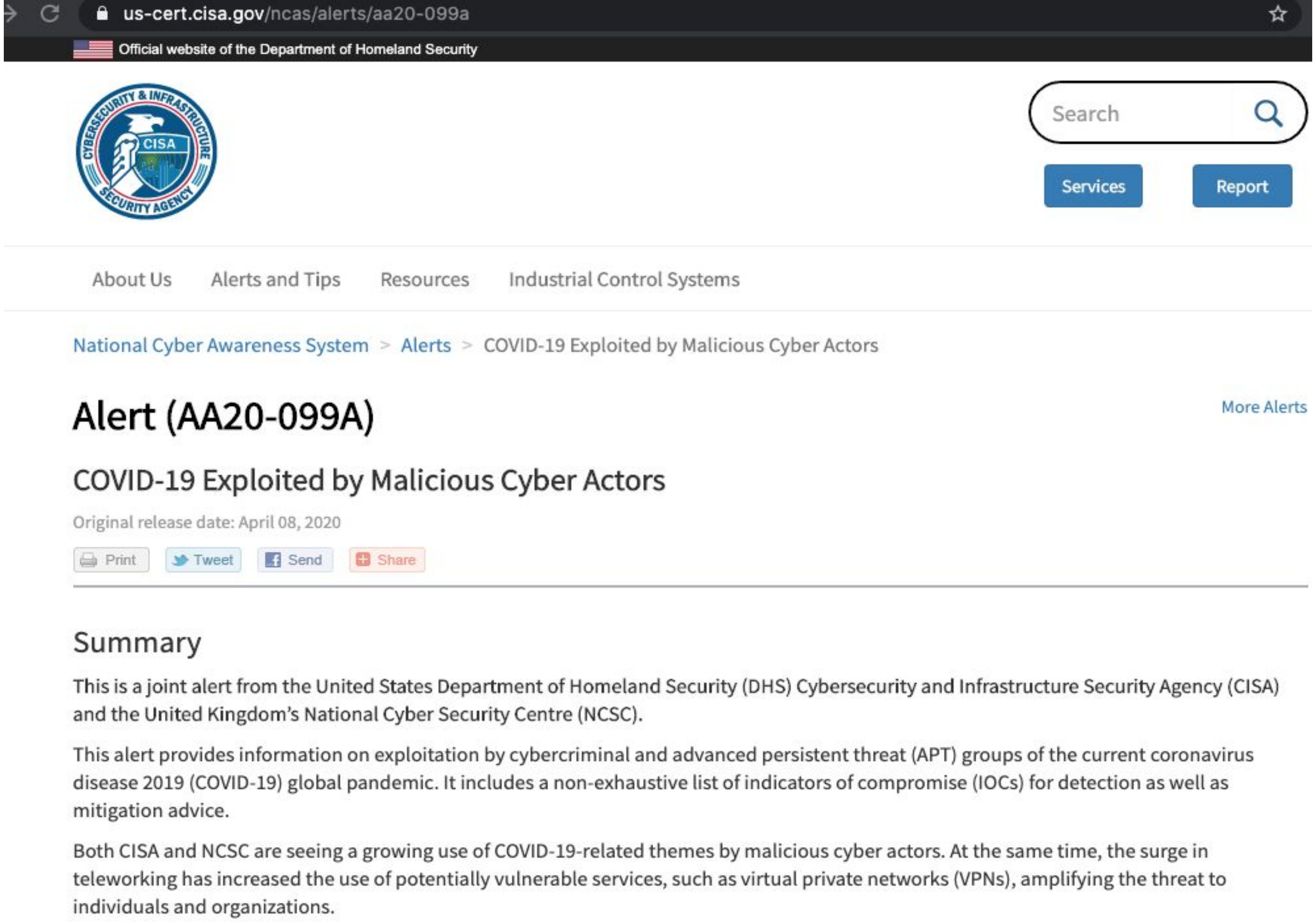
Local Field Office Locations: www.fbi.gov/contact-us/field

IMPLEMENTATION OF FRAUDULENT COVID-19 SHIPPING AND INSURANCE FEES BY CRIMINAL ACTORS

The Federal Bureau of Investigation (FBI) is issuing this announcement to raise awareness of criminal actors exploiting the public and the shipping industry by invoking fake COVID-19-related regulations and fees.

The FBI is aware of incidents involving individuals or companies referencing fake "newly enacted" COVID-19 shipping laws, regulations, or insurance requirements with the purpose of charging additional fees before the delivery of a product. Examples of this criminal activity include demanding fraudulent COVID-19 insurance fees after the purchase for the delivery of live pets from online U.S. websites. An additional example includes criminal actors fraudulently collecting "refundable" maritime insurance fees, citing fake COVID-19 laws.

Source: https://www.ic3.gov/media/2020/200611.aspx



us-cert.cisa.gov/ncas/alerts/aa20-099a
Official website of the Department of Homeland Security
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
Search
Services
Report
About Us
Alerts and Tips
Resources
Industrial Control Systems
National Cyber Awareness System > Alerts > COVID-19 Exploited by Malicious Cyber Actors
More Alerts
Print
Tweet
Send
Share

Alert (AA20-099A)

COVID-19 Exploited by Malicious Cyber Actors

Original release date: April 08, 2020

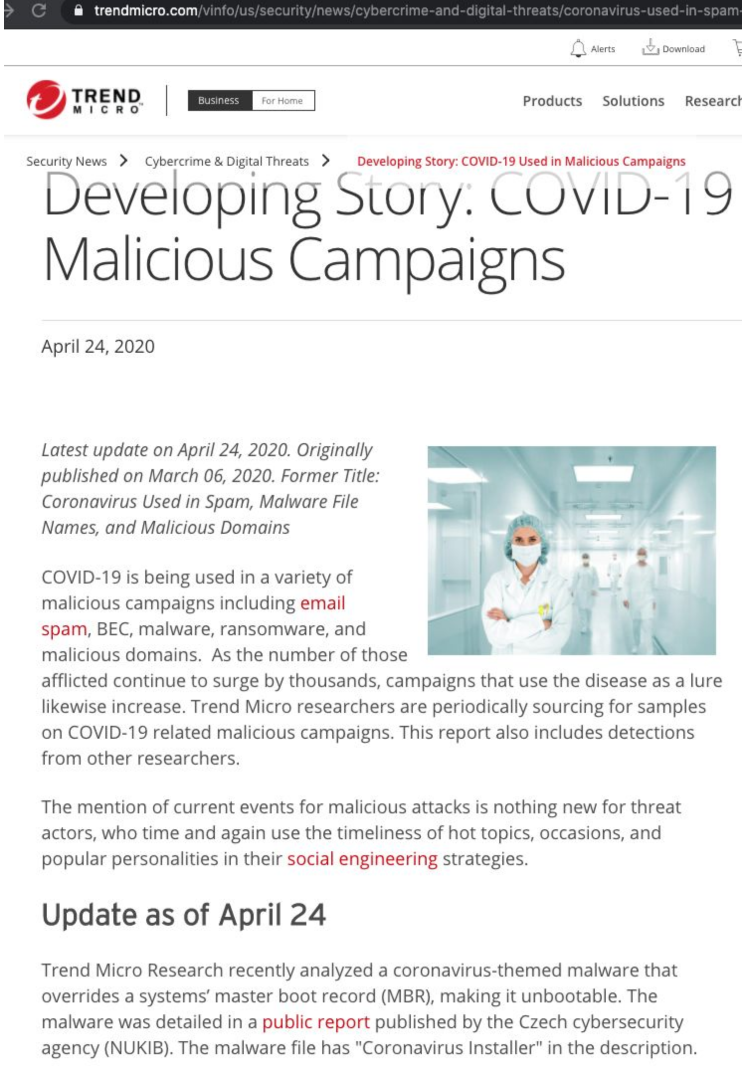
Summary

This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

Source: https://us-cert.cisa.gov/ncas/alerts/aa20-099a


trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-
Alerts
Download
TREND MICRO
Business
For Home
Products
Solutions
Researc
Security News
Cybercrime & Digital Threats
Developing Story: COVID-19 Used in Malicious Campaigns

Developing Story: COVID-19 Malicious Campaigns

April 24, 2020

Latest update on April 24, 2020. Originally published on March 06, 2020. Former Title: Coronavirus Used in Spam, Malware File Names, and Malicious Domains

COVID-19 is being used in a variety of malicious campaigns including email spam, BEC, malware, ransomware, and malicious domains. As the number of those afflicted continue to surge by thousands, campaigns that use the disease as a lure likewise increase. Trend Micro researchers are periodically sourcing for samples on COVID-19 related malicious campaigns. This report also includes detections from other researchers.

The mention of current events for malicious attacks is nothing new for threat actors, who time and again use the timeliness of hot topics, occasions, and popular personalities in their social engineering strategies.

Update as of April 24

Trend Micro Research recently analyzed a coronavirus-themed malware that overrides a systems' master boot record (MBR), making it unbootable. The malware was detailed in a public report published by the Czech cybersecurity agency (NUKIB). The malware file has "Coronavirus Installer" in the description.

Source: link

We also parsed data from Trend Micro's Smart Protection Network and found more information about the variety of threats using COVID-19 to manipulate targets. As seen in the image below, spam is the main offender. Almost 70% of all the threats leveraging the virus were spam messages.

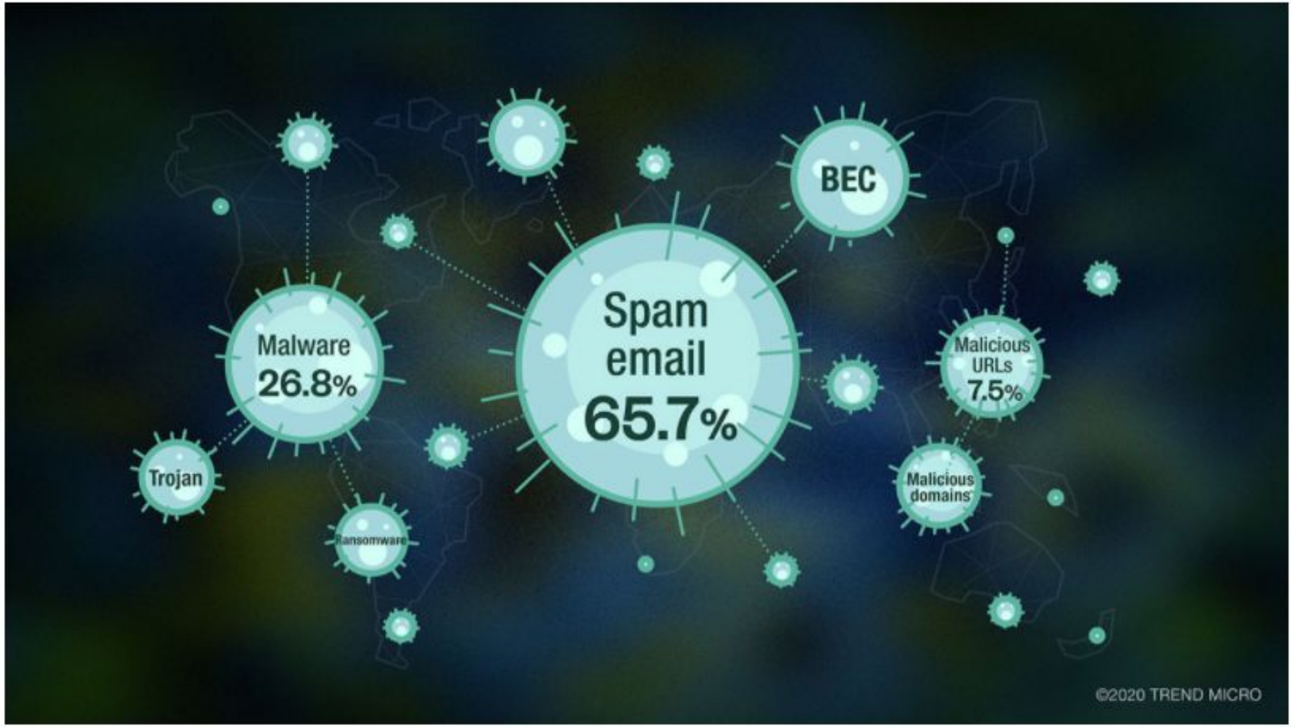
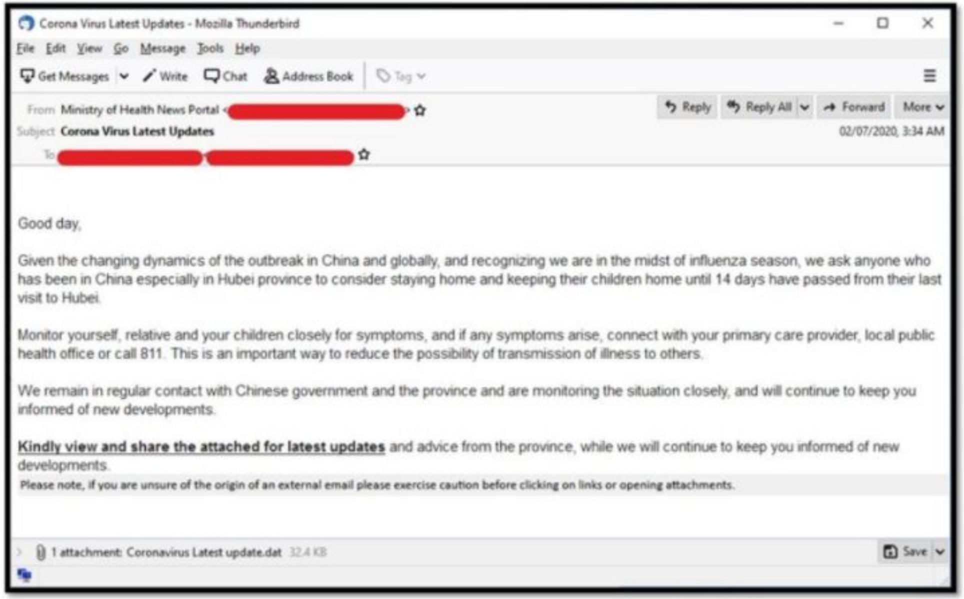


Figure 4. Map of threats using COVID-19

Types of Threats Using COVID-19

Spam

Many aspects of daily work, from meetings to presentations and collaborative tasks, have moved online because of quarantine restrictions affecting offices across the globe. As users adapt to new methods of working, they should be wary of cybercriminals using popular online tools, sharing software, and file attachments in their scams. Our Email Reputation Services team found coronavirus-related emails with malicious attachments sent to users as early as February 2020.


Corona Virus Latest Updates - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
Save

From Ministry of Health News Portal <[redacted]>
Subject Corona Virus Latest Updates
02/07/2020, 3:34 AM
To [redacted] [redacted]

Good day,

Given the changing dynamics of the outbreak in China and globally, and recognizing we are in the midst of influenza season, we ask anyone who has been in China especially in Hubei province to consider staying home and keeping their children home until 14 days have passed from their last visit to Hubei.

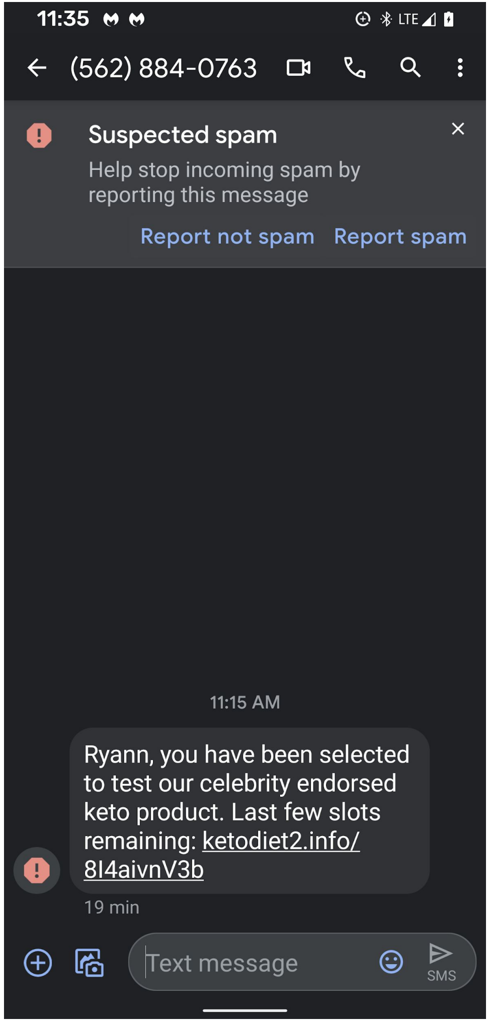
Monitor yourself, relative and your children closely for symptoms, and if any symptoms arise, connect with your primary care provider, local public health office or call 811. This is an important way to reduce the possibility of transmission of illness to others.

We remain in regular contact with Chinese government and the province and are monitoring the situation closely, and will continue to keep you informed of new developments.

Kindly view and share the attached for latest updates and advice from the province, while we will continue to keep you informed of new developments.

Please note, if you are unsure of the origin of an external email please exercise caution before clicking on links or opening attachments.

1 attachment: Coronavirus Latest update.dat 32.4 KB



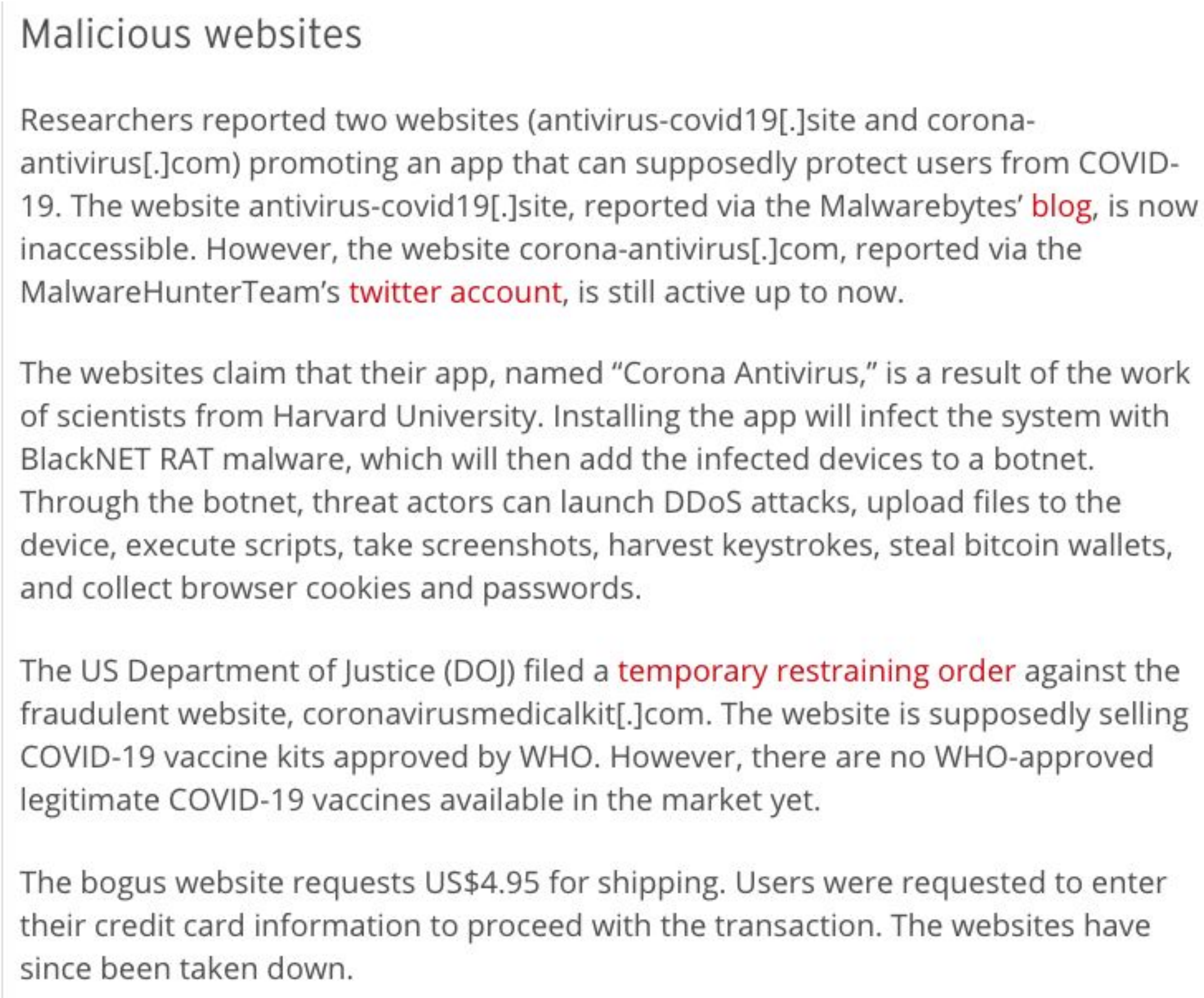
Suspected spam

Help stop incoming spam by reporting this message

11:15 AM

Ryann, you have been selected to test our celebrity endorsed keto product. Last few slots remaining: ketodiet2.info/8I4aivnV3b

19 min



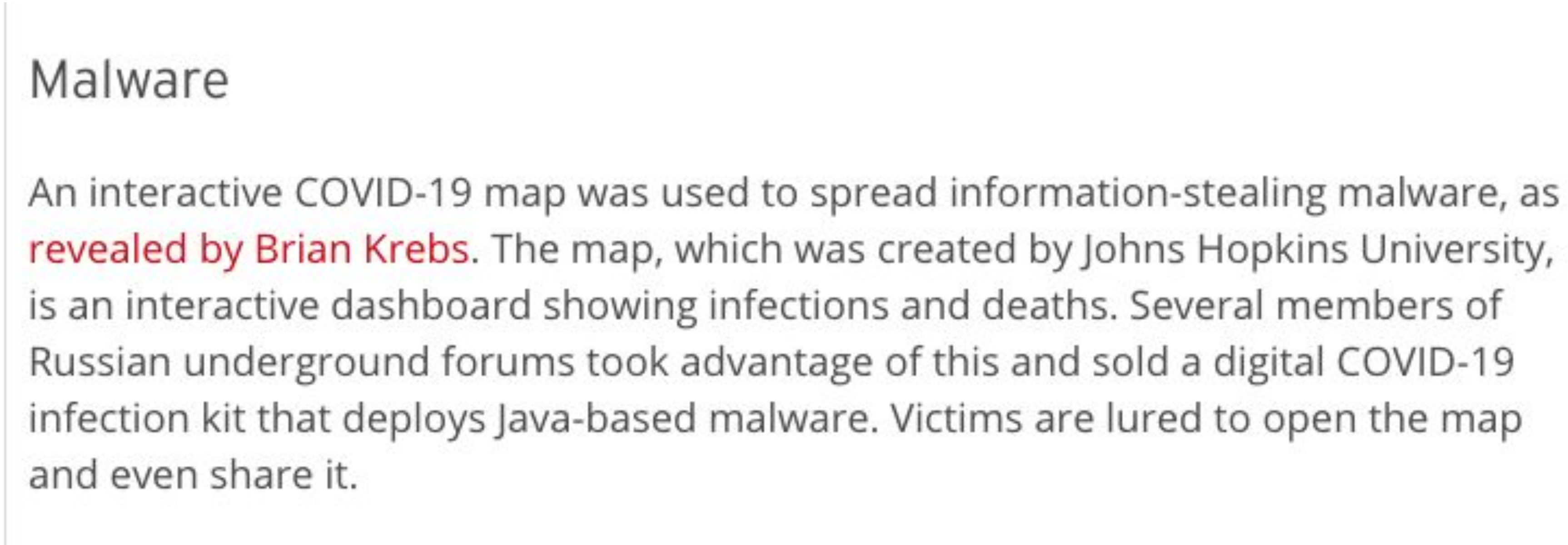
Malicious websites

Researchers reported two websites (antivirus-covid19[.]site and corona-antivirus[.]com) promoting an app that can supposedly protect users from COVID-19. The website antivirus-covid19[.]site, reported via the Malwarebytes' blog, is now inaccessible. However, the website corona-antivirus[.]com, reported via the MalwareHunterTeam's twitter account, is still active up to now.

The websites claim that their app, named "Corona Antivirus," is a result of the work of scientists from Harvard University. Installing the app will infect the system with BlackNET RAT malware, which will then add the infected devices to a botnet. Through the botnet, threat actors can launch DDoS attacks, upload files to the device, execute scripts, take screenshots, harvest keystrokes, steal bitcoin wallets, and collect browser cookies and passwords.

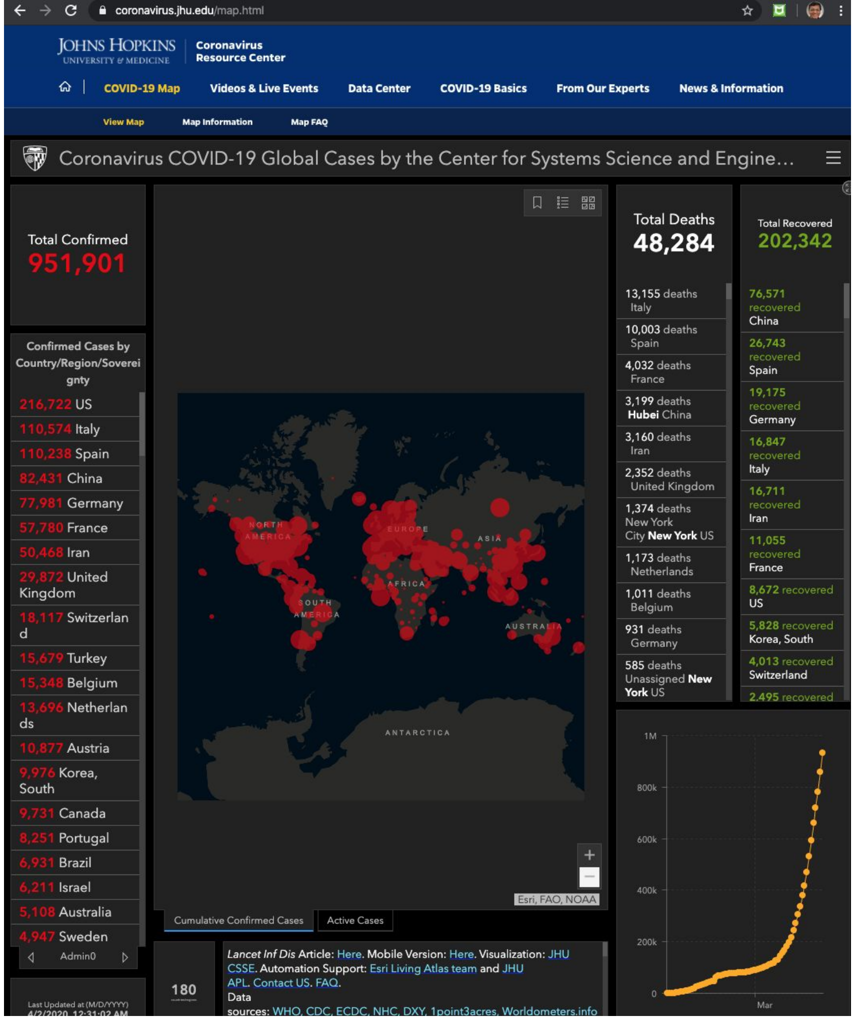
The US Department of Justice (DOJ) filed a temporary restraining order against the fraudulent website, coronavirusmedicalkit[.]com. The website is supposedly selling COVID-19 vaccine kits approved by WHO. However, there are no WHO-approved legitimate COVID-19 vaccines available in the market yet.

The bogus website requests US$4.95 for shipping. Users were requested to enter their credit card information to proceed with the transaction. The websites have since been taken down.



Malware

An interactive COVID-19 map was used to spread information-stealing malware, as revealed by Brian Krebs. The map, which was created by Johns Hopkins University, is an interactive dashboard showing infections and deaths. Several members of Russian underground forums took advantage of this and sold a digital COVID-19 infection kit that deploys Java-based malware. Victims are lured to open the map and even share it.



Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engine…

Total Confirmed
951,901

Confirmed Cases by Country/Region/Sovereignty

216,722	US
110,574	Italy
110,238	Spain
82,431	China
77,981	Germany
57,780	France
50,468	Iran
29,872	United Kingdom
18,117	Switzerland
15,679	Turkey
15,348	Belgium
13,696	Netherlands
10,877	Austria
9,976	Korea, South
9,731	Canada
8,251	Portugal
6,931	Brazil
6,211	Israel
5,108	Australia
4,947	Sweden

Last Updated at (M/D/YYYY)
4/2/2020 12:31:02 AM

Total Deaths
48,284

13,155 deaths	Italy
10,003 deaths	Spain
4,032 deaths	France
3,199 deaths	**Hubei** China
3,160 deaths	Iran
2,352 deaths	United Kingdom
1,374 deaths	New York City **New York** US
1,173 deaths	Netherlands
1,011 deaths	Belgium
931 deaths	Germany
585 deaths	Unassigned **New York** US

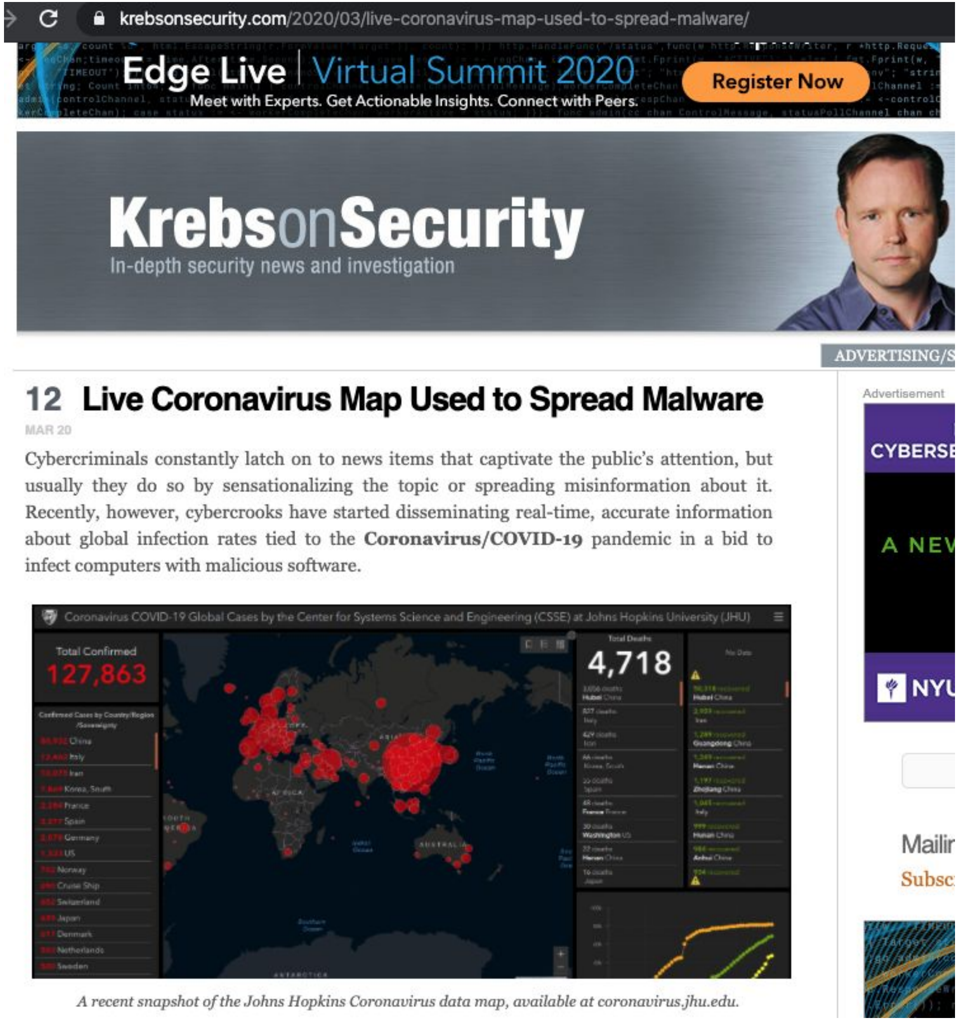
Total Recovered
202,342

76,571 recovered	China
26,743 recovered	Spain
19,175 recovered	Germany
16,847 recovered	Italy
16,711 recovered	Iran
11,055 recovered	France
8,672 recovered	US
5,828 recovered	Korea, South
4,013 recovered	Switzerland
2,495 recovered	

Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Esri Living Atlas team and JHU APL. Contact US. FAQ.

Data sources: WHO, CDC, ECDC, NHC, DXY, 1point3acres, Worldometers.info

Source: Official Johns Hopkins Map https://coronavirus.jhu.edu/map.html


krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

KrebsonSecurity
In-depth security news and investigation
ADVERTISING/S

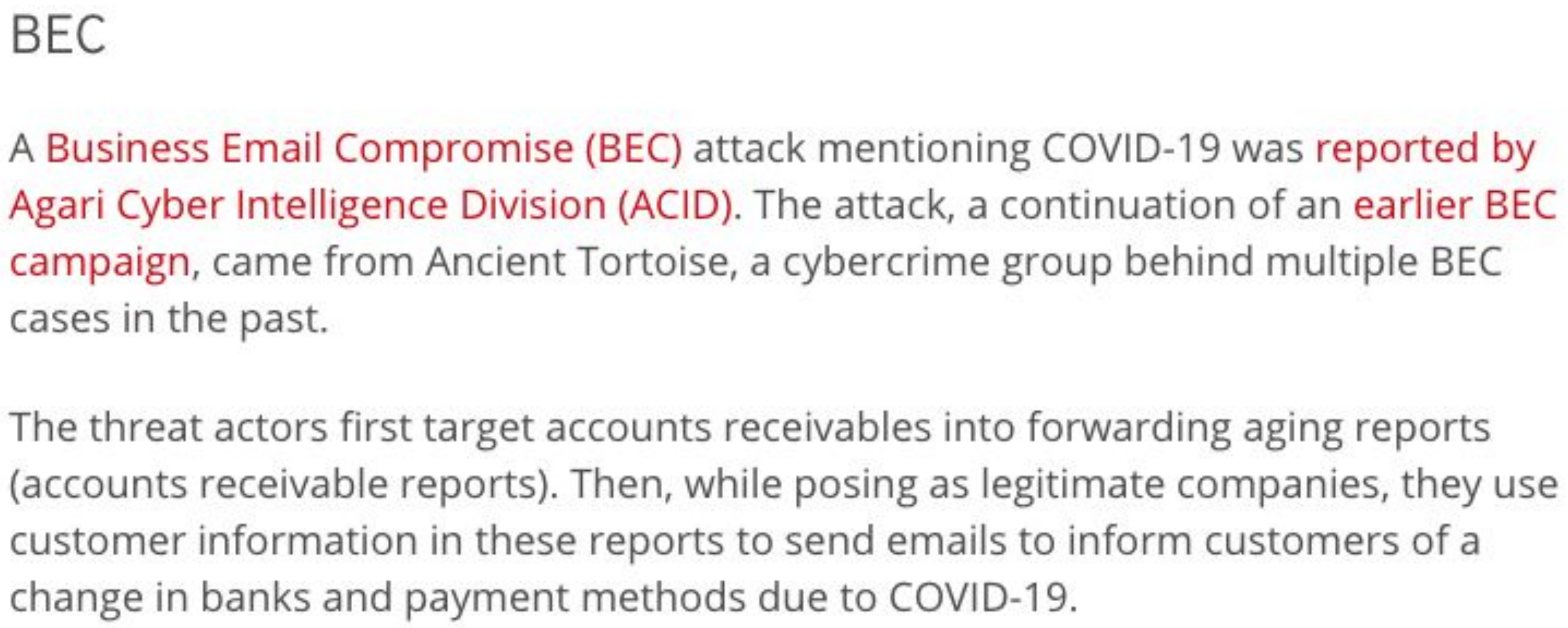
12 Live Coronavirus Map Used to Spread Malware

MAR 20

Cybercriminals constantly latch on to news items that captivate the public's attention, but usually they do so by sensationalizing the topic or spreading misinformation about it. Recently, however, cybercrooks have started disseminating real-time, accurate information about global infection rates tied to the **Coronavirus/COVID-19** pandemic in a bid to infect computers with malicious software.

Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)
Total Confirmed
127,863
Total Deaths
4,718

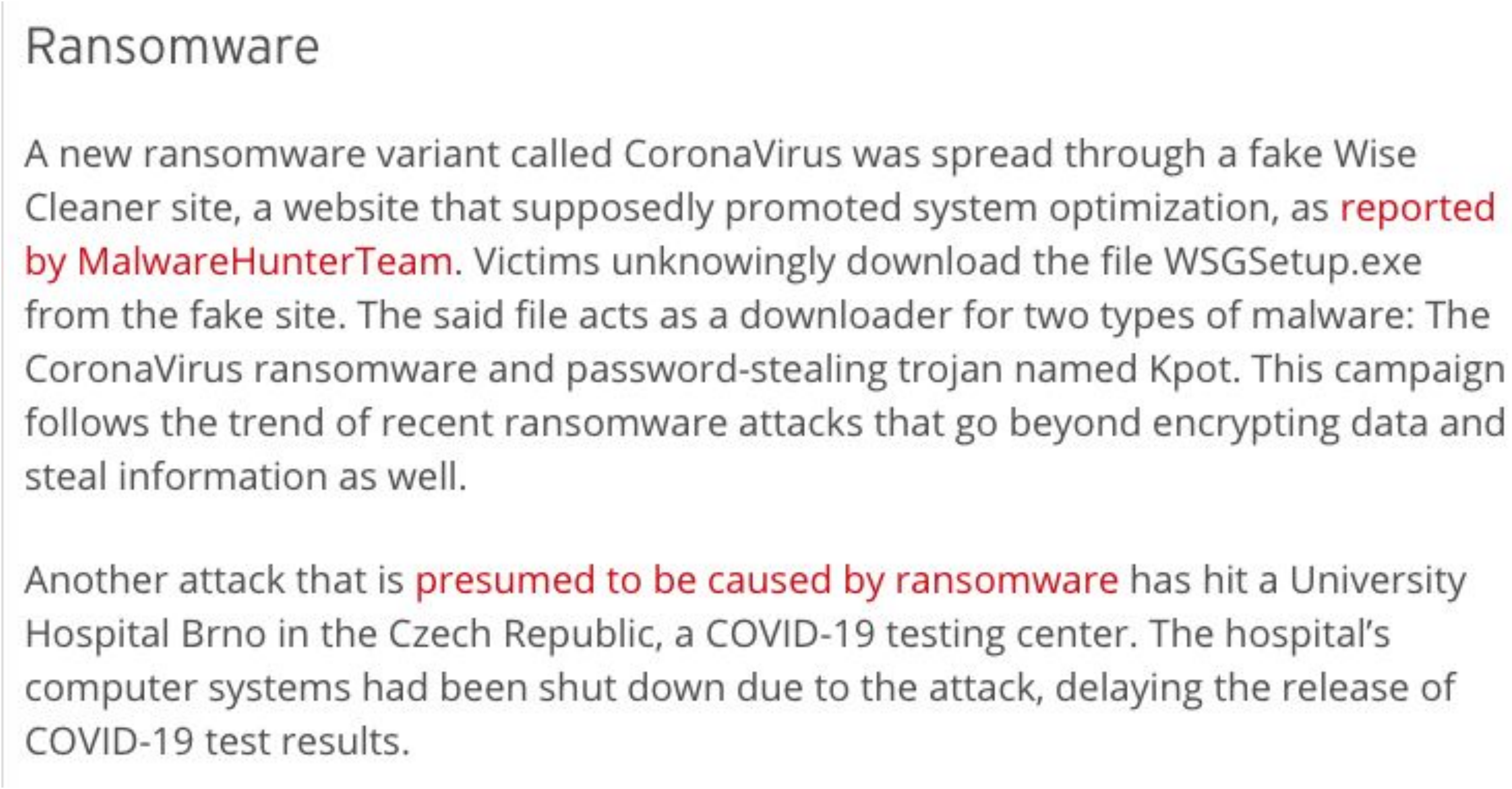
A recent snapshot of the Johns Hopkins Coronavirus data map, available at coronavirus.jhu.edu.



BEC

A Business Email Compromise (BEC) attack mentioning COVID-19 was reported by Agari Cyber Intelligence Division (ACID). The attack, a continuation of an earlier BEC campaign, came from Ancient Tortoise, a cybercrime group behind multiple BEC cases in the past.

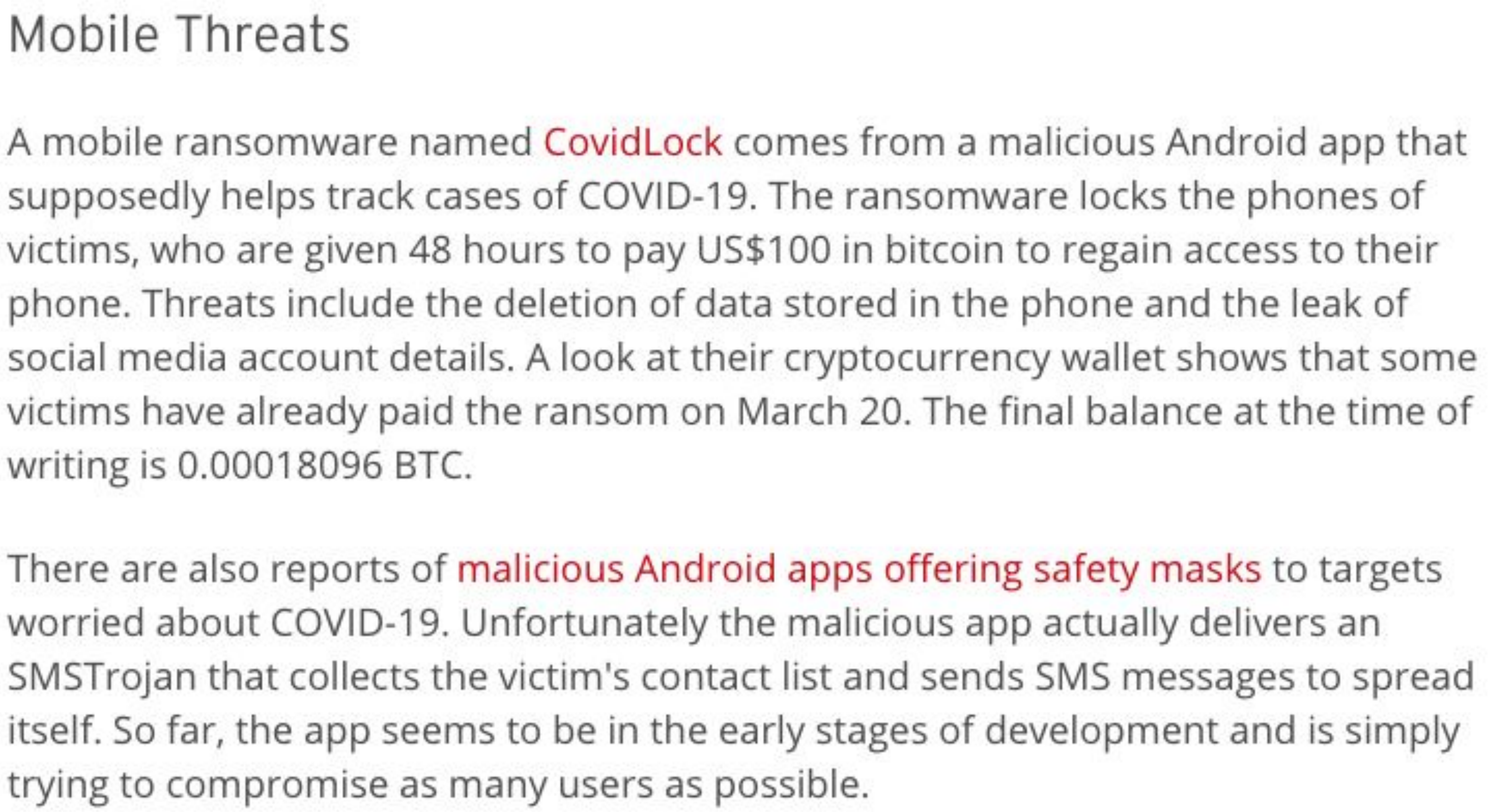
The threat actors first target accounts receivables into forwarding aging reports (accounts receivable reports). Then, while posing as legitimate companies, they use customer information in these reports to send emails to inform customers of a change in banks and payment methods due to COVID-19.



Ransomware

A new ransomware variant called CoronaVirus was spread through a fake Wise Cleaner site, a website that supposedly promoted system optimization, as reported by MalwareHunterTeam. Victims unknowingly download the file WSGSetup.exe from the fake site. The said file acts as a downloader for two types of malware: The CoronaVirus ransomware and password-stealing trojan named Kpot. This campaign follows the trend of recent ransomware attacks that go beyond encrypting data and steal information as well.

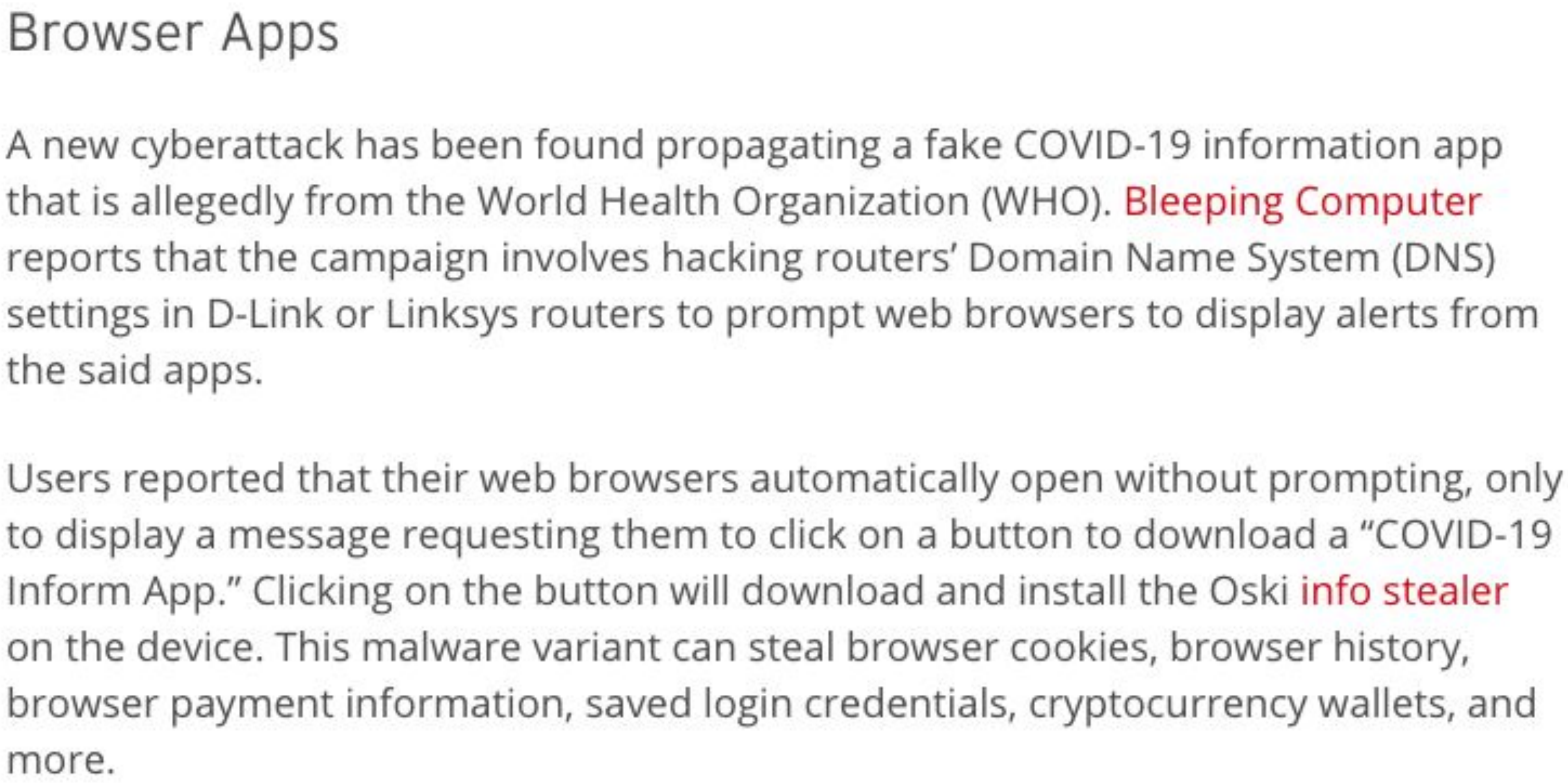
Another attack that is presumed to be caused by ransomware has hit a University Hospital Brno in the Czech Republic, a COVID-19 testing center. The hospital's computer systems had been shut down due to the attack, delaying the release of COVID-19 test results.



Mobile Threats

A mobile ransomware named CovidLock comes from a malicious Android app that supposedly helps track cases of COVID-19. The ransomware locks the phones of victims, who are given 48 hours to pay US$100 in bitcoin to regain access to their phone. Threats include the deletion of data stored in the phone and the leak of social media account details. A look at their cryptocurrency wallet shows that some victims have already paid the ransom on March 20. The final balance at the time of writing is 0.00018096 BTC.

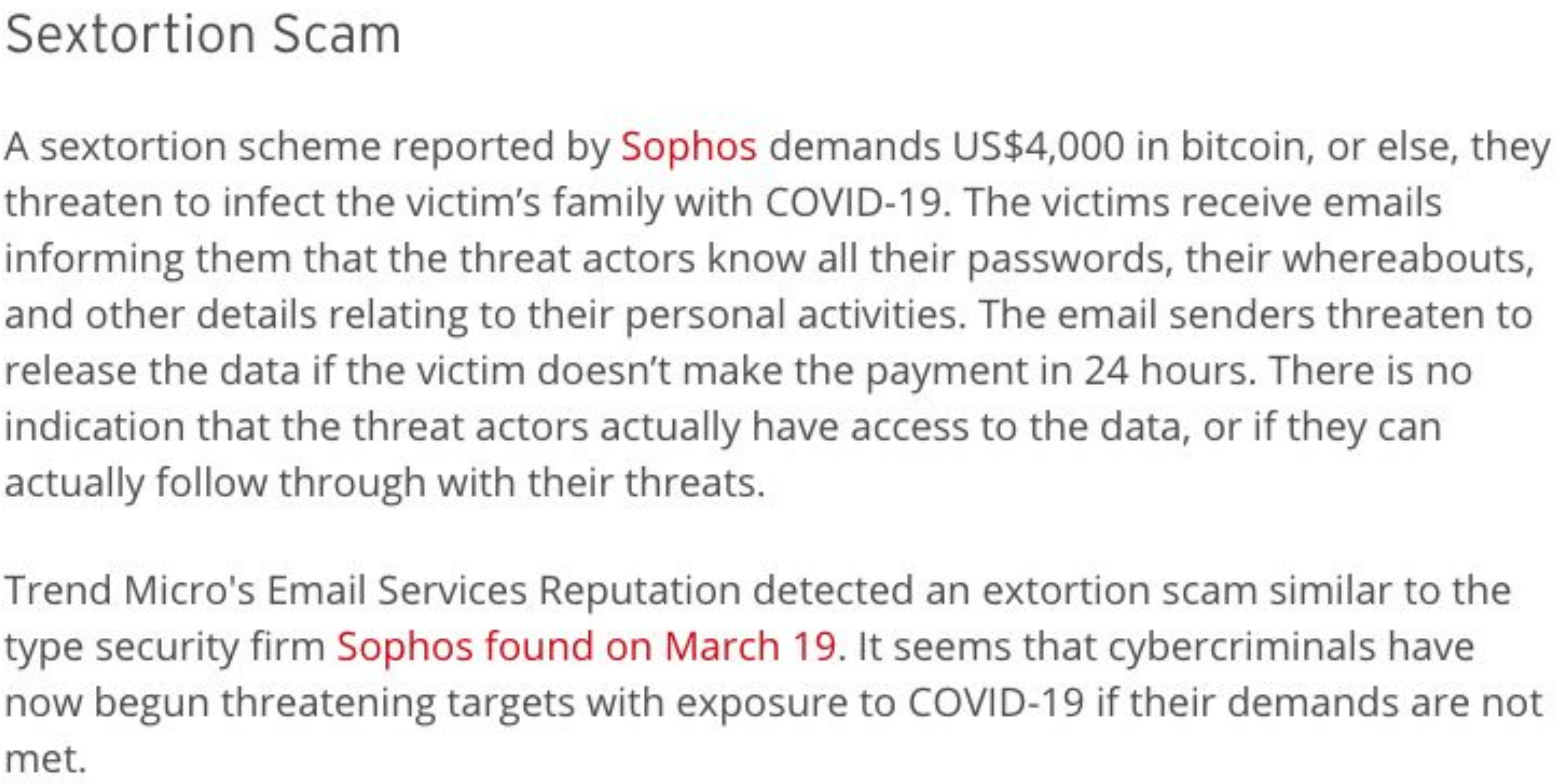
There are also reports of malicious Android apps offering safety masks to targets worried about COVID-19. Unfortunately the malicious app actually delivers an SMSTrojan that collects the victim's contact list and sends SMS messages to spread itself. So far, the app seems to be in the early stages of development and is simply trying to compromise as many users as possible.



Browser Apps

A new cyberattack has been found propagating a fake COVID-19 information app that is allegedly from the World Health Organization (WHO). Bleeping Computer reports that the campaign involves hacking routers' Domain Name System (DNS) settings in D-Link or Linksys routers to prompt web browsers to display alerts from the said apps.

Users reported that their web browsers automatically open without prompting, only to display a message requesting them to click on a button to download a "COVID-19 Inform App." Clicking on the button will download and install the Oski info stealer on the device. This malware variant can steal browser cookies, browser history, browser payment information, saved login credentials, cryptocurrency wallets, and more.



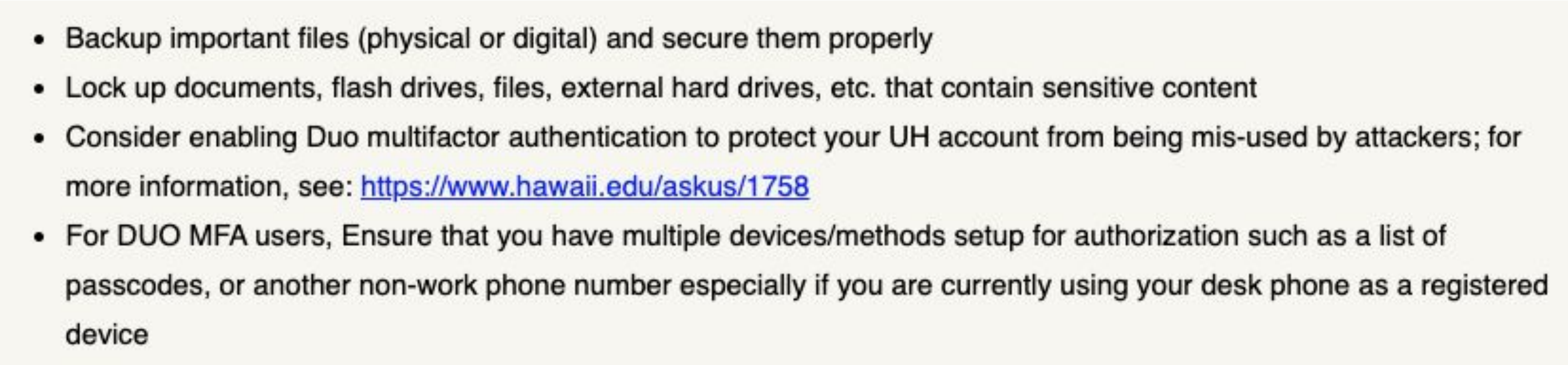
Sextortion Scam

A sextortion scheme reported by Sophos demands US$4,000 in bitcoin, or else, they threaten to infect the victim's family with COVID-19. The victims receive emails informing them that the threat actors know all their passwords, their whereabouts, and other details relating to their personal activities. The email senders threaten to release the data if the victim doesn't make the payment in 24 hours. There is no indication that the threat actors actually have access to the data, or if they can actually follow through with their threats.

Trend Micro's Email Services Reputation detected an extortion scam similar to the type security firm Sophos found on March 19. It seems that cybercriminals have now begun threatening targets with exposure to COVID-19 if their demands are not met.

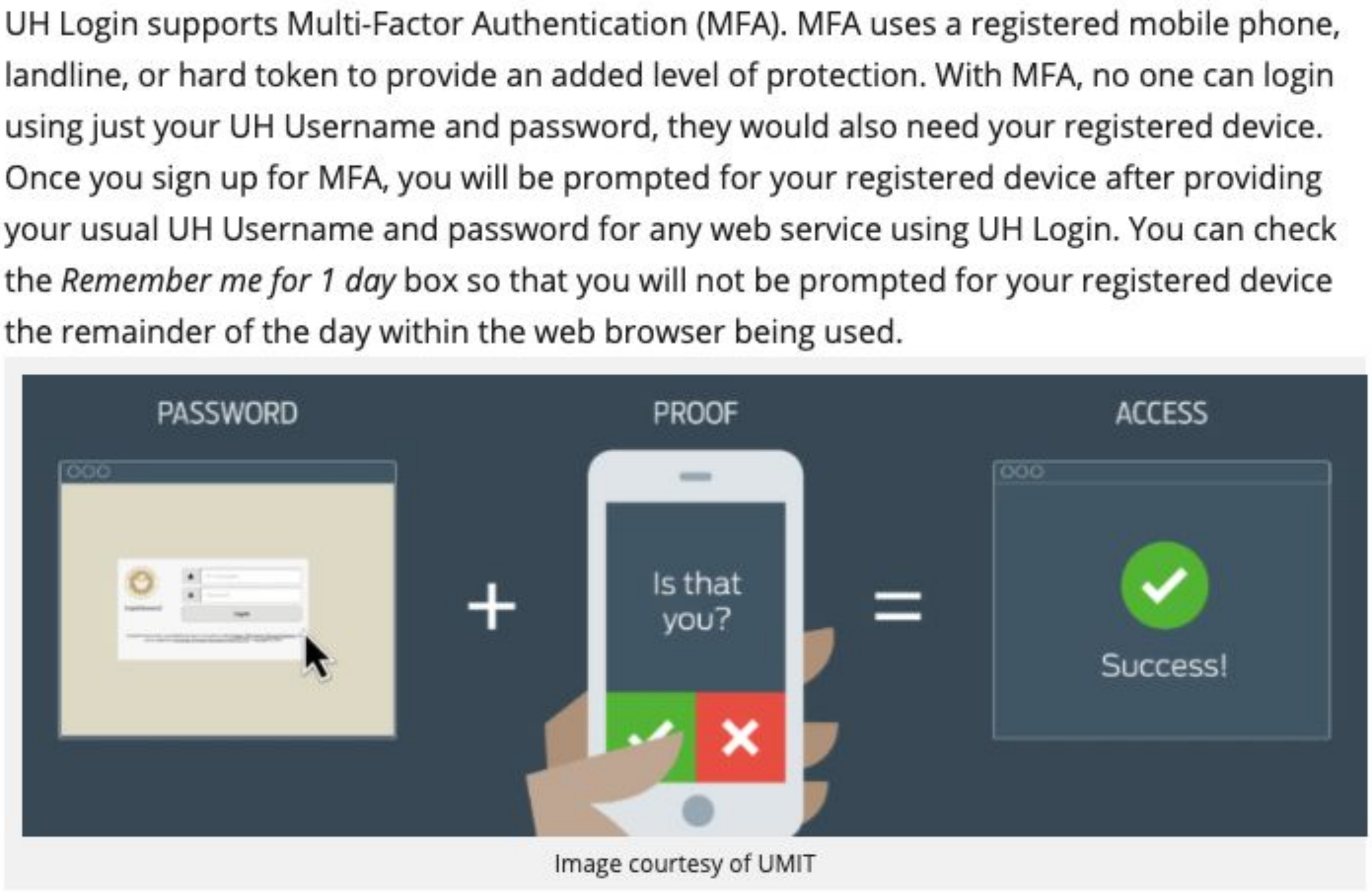
Secure Your Home Office!

Preparation - Setting up your secure office



- Backup important files (physical or digital) and secure them properly
- Lock up documents, flash drives, files, external hard drives, etc. that contain sensitive content
- Consider enabling Duo multifactor authentication to protect your UH account from being mis-used by attackers; for more information, see: https://www.hawaii.edu/askus/1758
- For DUO MFA users, Ensure that you have multiple devices/methods setup for authorization such as a list of passcodes, or another non-work phone number especially if you are currently using your desk phone as a registered device

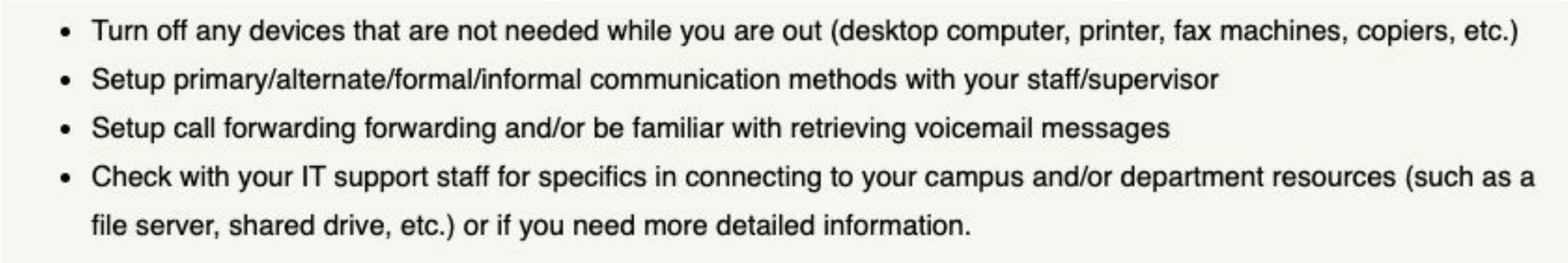
Use Multi-Factor Authentication



UH Login supports Multi-Factor Authentication (MFA). MFA uses a registered mobile phone, landline, or hard token to provide an added level of protection. With MFA, no one can login using just your UH Username and password, they would also need your registered device. Once you sign up for MFA, you will be prompted for your registered device after providing your usual UH Username and password for any web service using UH Login. You can check the *Remember me for 1 day* box so that you will not be prompted for your registered device the remainder of the day within the web browser being used.

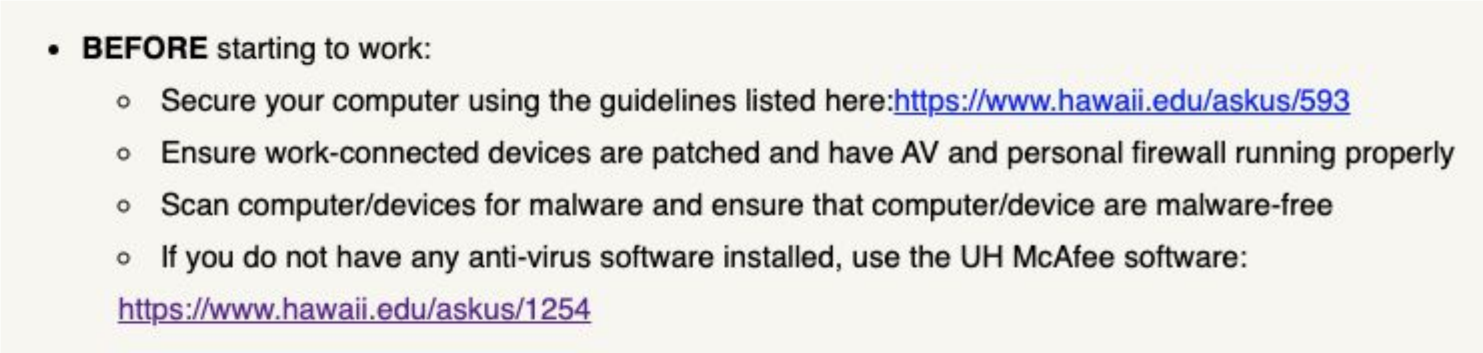
Image courtesy of UMIT

Preparation - Setting up your secure office



- Turn off any devices that are not needed while you are out (desktop computer, printer, fax machines, copiers, etc.)
- Setup primary/alternate/formal/informal communication methods with your staff/supervisor
- Setup call forwarding forwarding and/or be familiar with retrieving voicemail messages
- Check with your IT support staff for specifics in connecting to your campus and/or department resources (such as a file server, shared drive, etc.) or if you need more detailed information.

Preparation - Setting up your secure office



- **BEFORE** starting to work:
  - Secure your computer using the guidelines listed here:https://www.hawaii.edu/askus/593
  - Ensure work-connected devices are patched and have AV and personal firewall running properly
  - Scan computer/devices for malware and ensure that computer/device are malware-free
  - If you do not have any anti-virus software installed, use the UH McAfee software:

  https://www.hawaii.edu/askus/1254

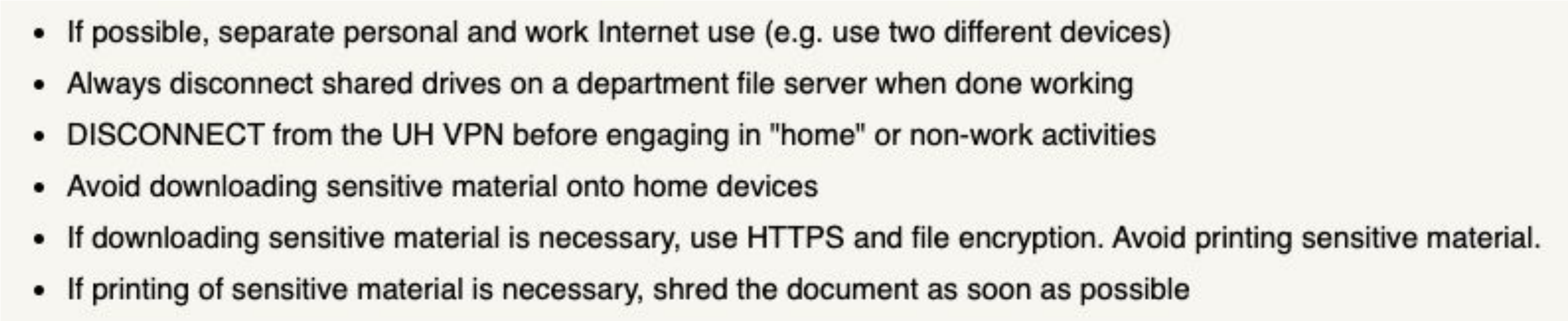
Tips!

1. Run Windows Update or update MacOS to latest version
2. Do a Full Hard Disk Scan of your Anti-Virus
3. Install and run Malwarebytes on your phone!
4. Encrypt your phone and setup screen lock
5. Turn on Firewall on your Windows or Mac

SAFEGUARD YOUR MOBILE EXPERIENCE

Protect your mobile devices and avoid annoying scams with Malwarebytes for iOS and Android.

Cyber Hygiene and Security Mindset

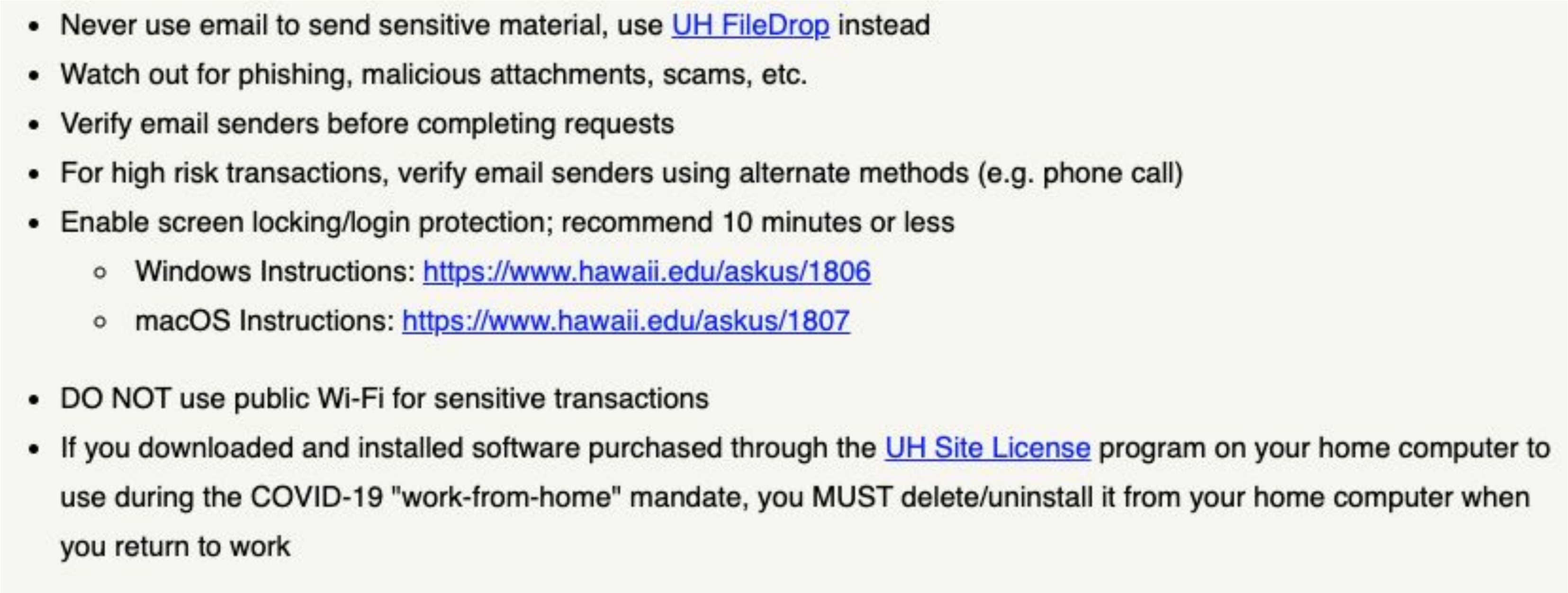


- If possible, separate personal and work Internet use (e.g. use two different devices)
- Always disconnect shared drives on a department file server when done working
- DISCONNECT from the UH VPN before engaging in "home" or non-work activities
- Avoid downloading sensitive material onto home devices
- If downloading sensitive material is necessary, use HTTPS and file encryption. Avoid printing sensitive material.
- If printing of sensitive material is necessary, shred the document as soon as possible

Tips!

1. If possible, keep work computer totally separate from home machines!
2. Buy or get a shredder! Shred anything with personal, banking info etc.
3. Disconnect from VPN or shared drives once you are done!
4. Turn off (not just log out) work computer after you are done with work.
5. Try to save directly to Google Drive, instead of downloading to local HD

Cyber Hygiene and Security Mindset



- Never use email to send sensitive material, use UH FileDrop instead
- Watch out for phishing, malicious attachments, scams, etc.
- Verify email senders before completing requests
- For high risk transactions, verify email senders using alternate methods (e.g. phone call)
- Enable screen locking/login protection; recommend 10 minutes or less
  - Windows Instructions: https://www.hawaii.edu/askus/1806
  - macOS Instructions: https://www.hawaii.edu/askus/1807
- DO NOT use public Wi-Fi for sensitive transactions
- If you downloaded and installed software purchased through the UH Site License program on your home computer to use during the COVID-19 "work-from-home" mandate, you MUST delete/uninstall it from your home computer when you return to work

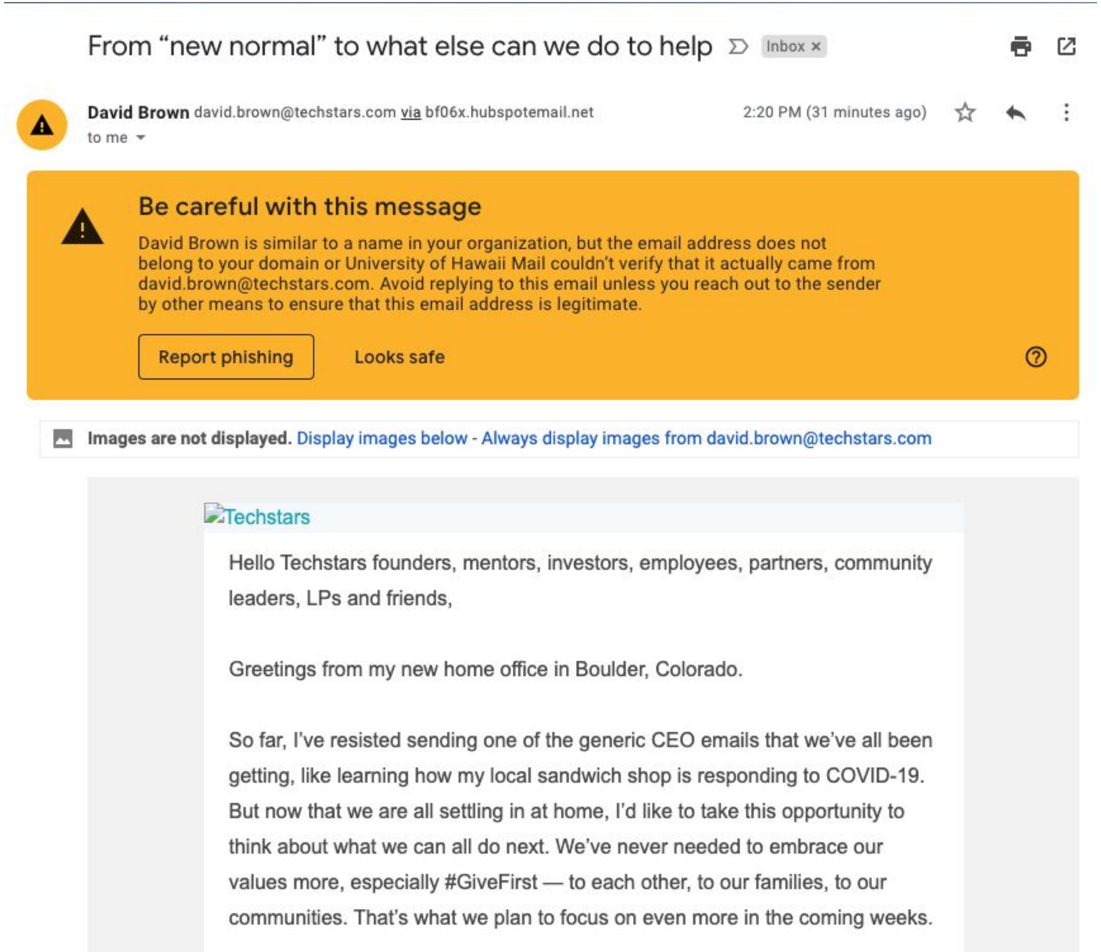
<u>Tips!</u>

1. If possible, keep work computer totally separate from home machines!
2. Buy or get a shredder! Shred anything with personal, banking info etc.
3. Setup work computer to lock screen after 10 minutes of inactivity.

Security Mindset - Sample Phishing Attempt

Trust but verify!

Gmail warns about many phishing attempts



From "new normal" to what else can we do to help

David Brown david.brown@techstars.com via bf06x.hubspotemail.net
to me

2:20 PM (31 minutes ago)

Be careful with this message

David Brown is similar to a name in your organization, but the email address does not belong to your domain or University of Hawaii Mail couldn't verify that it actually came from david.brown@techstars.com. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

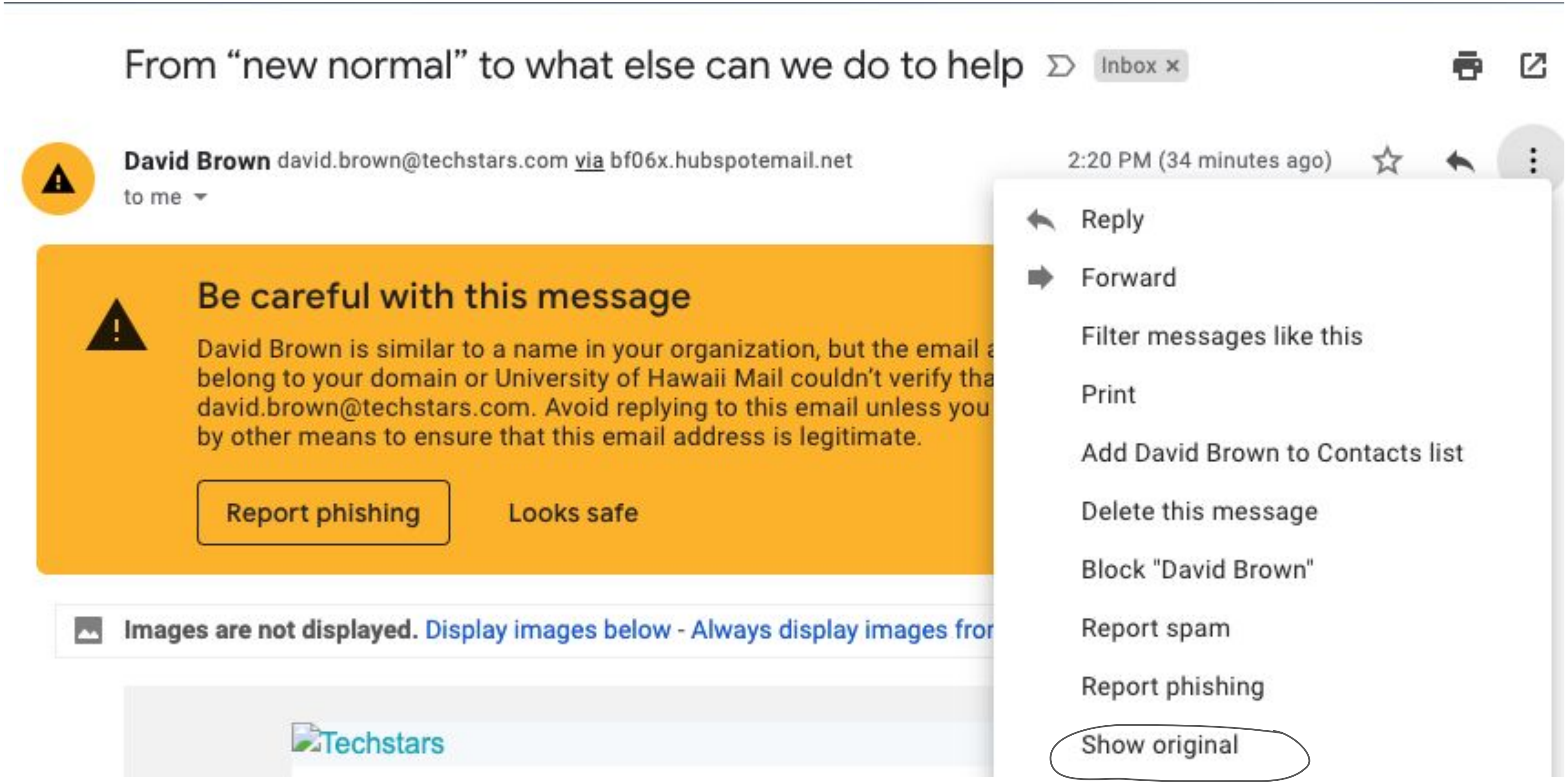
Images are not displayed. Display images below - Always display images from david.brown@techstars.com

Techstars

Hello Techstars founders, mentors, investors, employees, partners, community leaders, LPs and friends,

Greetings from my new home office in Boulder, Colorado.

So far, I've resisted sending one of the generic CEO emails that we've all been getting, like learning how my local sandwich shop is responding to COVID-19. But now that we are all settling in at home, I'd like to take this opportunity to think about what we can all do next. We've never needed to embrace our values more, especially #GiveFirst — to each other, to our families, to our communities. That's what we plan to focus on even more in the coming weeks.



From “new normal” to what else can we do to help

David Brown david.brown@techstars.com via bf06x.hubspotemail.net

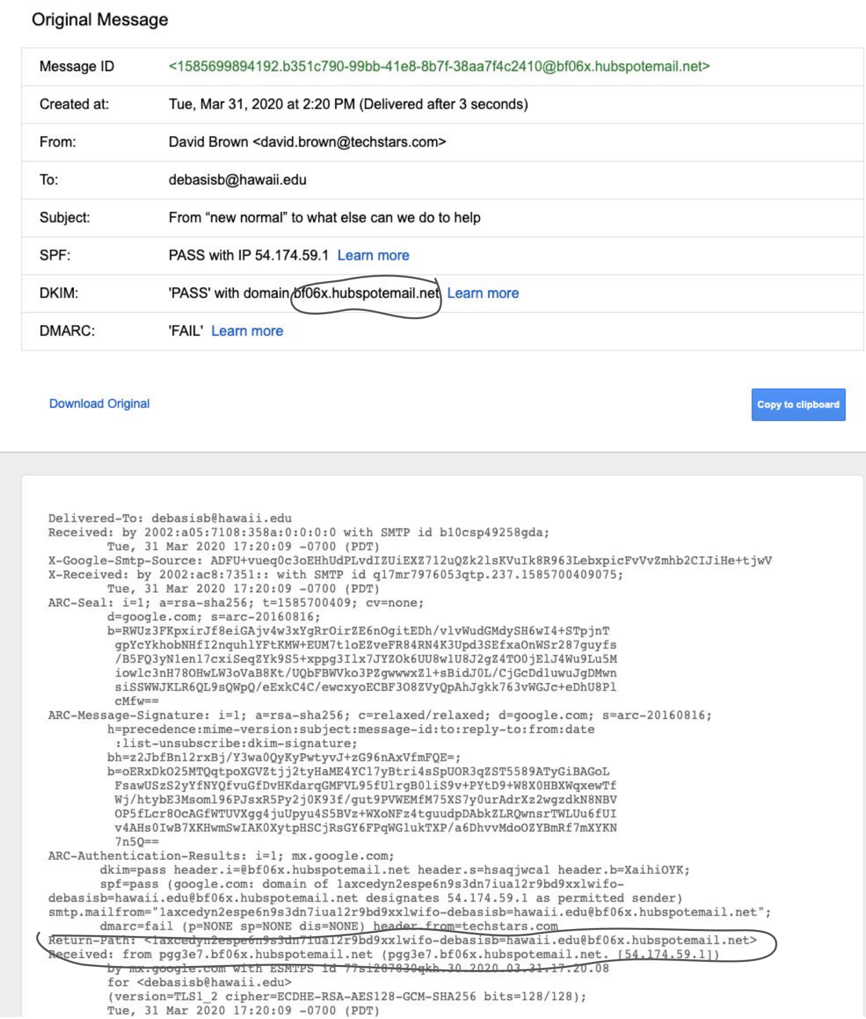
to me

2:20 PM (34 minutes ago)

Be careful with this message

David Brown is similar to a name in your organization, but the email a
belong to your domain or University of Hawaii Mail couldn't verify tha
david.brown@techstars.com. Avoid replying to this email unless you
by other means to ensure that this email address is legitimate.

Images are not displayed. Display images below - Always display images fro

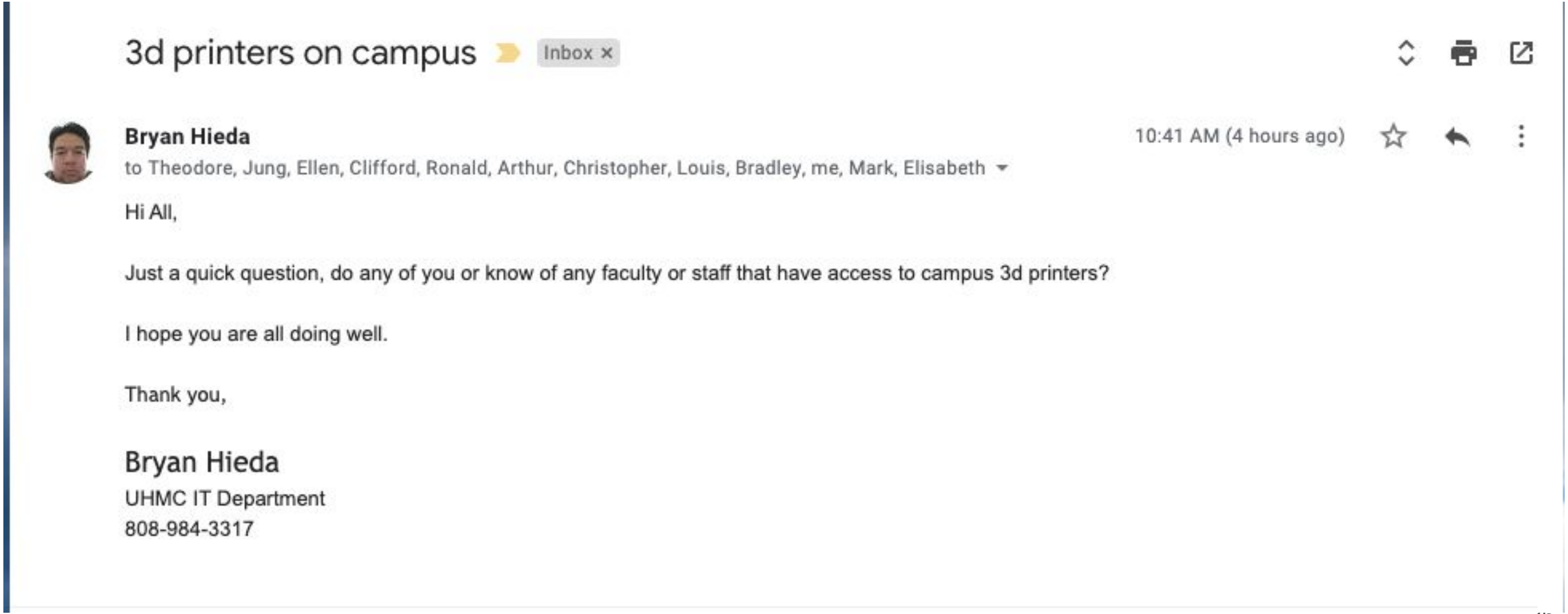


Original Message

Message ID	<1585699894192.b351c790-99bb-41e8-8b7f-38aa7f4c2410@bf06x.hubspotemail.net>
Created at:	Tue, Mar 31, 2020 at 2:20 PM (Delivered after 3 seconds)
From:	David Brown <david.brown@techstars.com>
To:	debasisb@hawaii.edu
Subject:	From “new normal” to what else can we do to help
SPF:	PASS with IP 54.174.59.1 Learn more
DKIM:	'PASS' with domain bf06x.hubspotemail.net Learn more
DMARC:	'FAIL' Learn more

```
Delivered-To: debasisb@hawaii.edu
Received: by 2002:a05:7108:358a:0:0:0:0 with SMTP id b10csp49258gda;
        Tue, 31 Mar 2020 17:20:09 -0700 (PDT)
X-Google-Smtp-Source: ADFU+vueq0c3oEHhUdPLvdIZUiEXZ712uQZk2lsKVuIk8R963LebxpicFvVvZmhb2CIJiHe+tjwV
X-Received: by 2002:ac8:7351:: with SMTP id q17mr7976053qtp.237.1585700409075;
        Tue, 31 Mar 2020 17:20:09 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1585700409; cv=none;
        d=google.com; s=arc-20160816;
        b=RWUz3FKpxirJf8eiGAjv4w3xYgRrOirZE6nOgitEDh/vlvWudGMdySH6wI4+STpjnT
         gpYcYkhobNHfI2nquhlYFtKMW+EUM7t1oEZveFR84RN4K3Upd3SEfxaOnWSr287guyfs
         /B5FQ3yN1en17cxiSeqZYk9S5+xppg3Ilx7JYZOk6UU8w1U8J2gZ4TO0jElJ4Wu9Lu5M
         iowlc3nH78OHwLW3oVaB8Kt/UQbFBWVko3PZgwwwxZl+sBidJ0L/CjGcDd1uwuJgDMwn
         siSSWWJKLR6QL9sQWpQ/eExkC4C/ewcxyoECBF3O8ZVyQpAhJgkk763vWGJc+eDhU8Pl
         cMfw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=precedence:mime-version:subject:message-id:to:reply-to:from:date
         :list-unsubscribe:dkim-signature;
        bh=z2JbfBn12rxBj/Y3wa0QyKyPwtyvJ+zG96nAxVfmFQE=;
        b=oERxDkO25MTQqtpoXGVZtjj2tyHaME4YC17yBtri4sSpUOR3qZST5589ATyGiBAGoL
         FsawUSzS2yYfNYQfvuGfDvHKdarqGMFVL95fUlrgB0liS9v+PYtD9+W8X0HBXWqxewTf
         Wj/htybE3Msoml96PJsxR5Py2j0K93f/gut9PVWEMfM75XS7y0urAdrXz2wgzdkN8NBV
         OP5fLcr8OcAGfWTUVXgg4juUpyu4S5BVz+WXoNFz4tguudpDAbkZLRQwnsrTWLUu6fUI
         v4AHs0IwB7XKHwmSwIAK0XytpHSCjRsGY6FPqWG1ukTXP/a6DhvvMdoOZYBmRf7mXYKN
         7n5Q==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@bf06x.hubspotemail.net header.s=hsaqjwca1 header.b=XaihiOYK;
       spf=pass (google.com: domain of 1axcedyn2espe6n9s3dn7iua12r9bd9xxlwifo-
debasisb=hawaii.edu@bf06x.hubspotemail.net designates 54.174.59.1 as permitted sender)
smtp.mailfrom="1axcedyn2espe6n9s3dn7iua12r9bd9xxlwifo-debasisb=hawaii.edu@bf06x.hubspotemail.net";
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=techstars.com
Return-Path: <1axcedyn2espe6n9s3dn7iua12r9bd9xxlwifo-debasisb=hawaii.edu@bf06x.hubspotemail.net>
Received: from pgg3e7.bf06x.hubspotemail.net (pgg3e7.bf06x.hubspotemail.net. [54.174.59.1])
        by mx.google.com with ESMTPS id 77si287830qkh.30.2020.03.31.17.20.08
        for <debasisb@hawaii.edu>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 31 Mar 2020 17:20:09 -0700 (PDT)
```

Spear Phishing?



Bryan Hieda
to Theodore, Jung, Ellen, Clifford, Ronald, Arthur, Christopher, Louis, Bradley, me, Mark, Elisabeth

10:41 AM (4 hours ago)

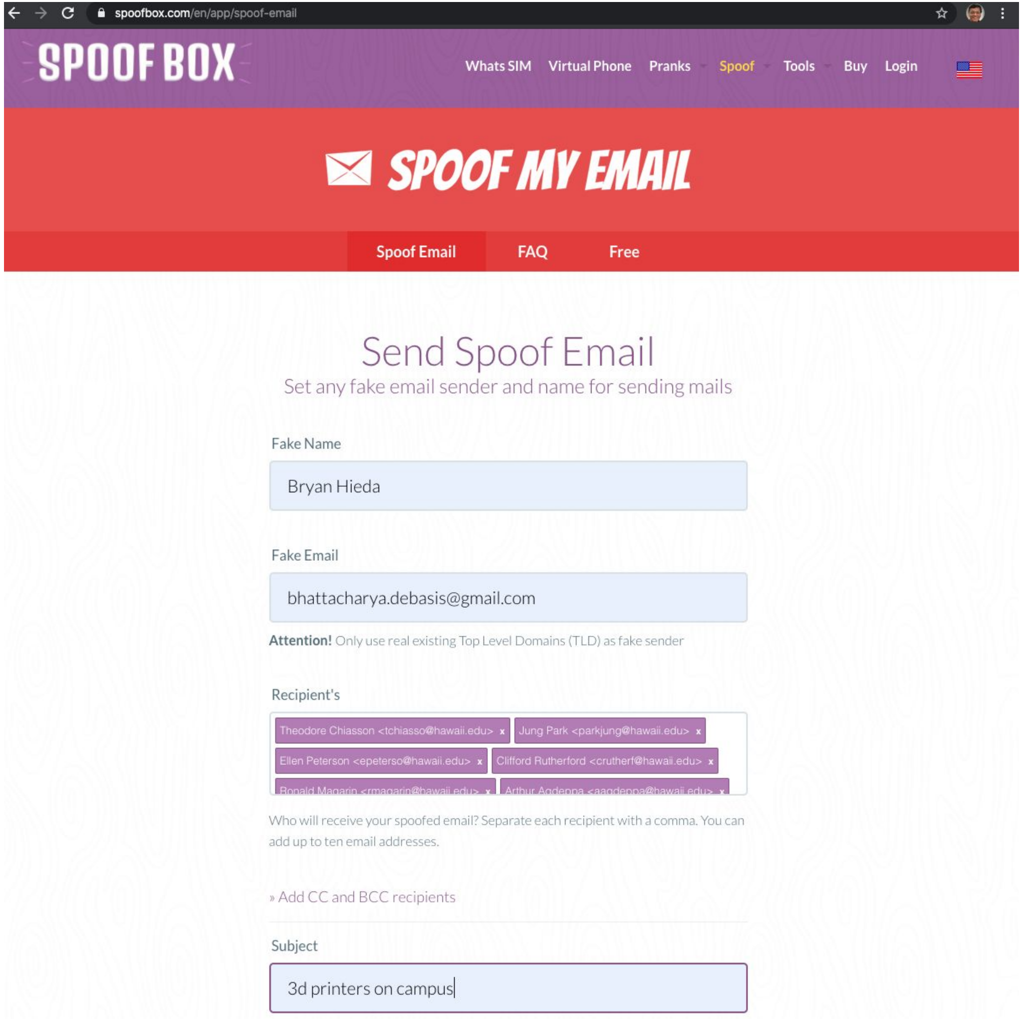
Hi All,

Just a quick question, do any of you or know of any faculty or staff that have access to campus 3d printers?

I hope you are all doing well.

Thank you,

Bryan Hieda
UHMC IT Department
808-984-3317



Send Spoof Email

Set any fake email sender and name for sending mails

Fake Name

Bryan Hieda

Fake Email

bhattacharya.debasis@gmail.com

Attention! Only use real existing Top Level Domains (TLD) as fake sender

Recipient's

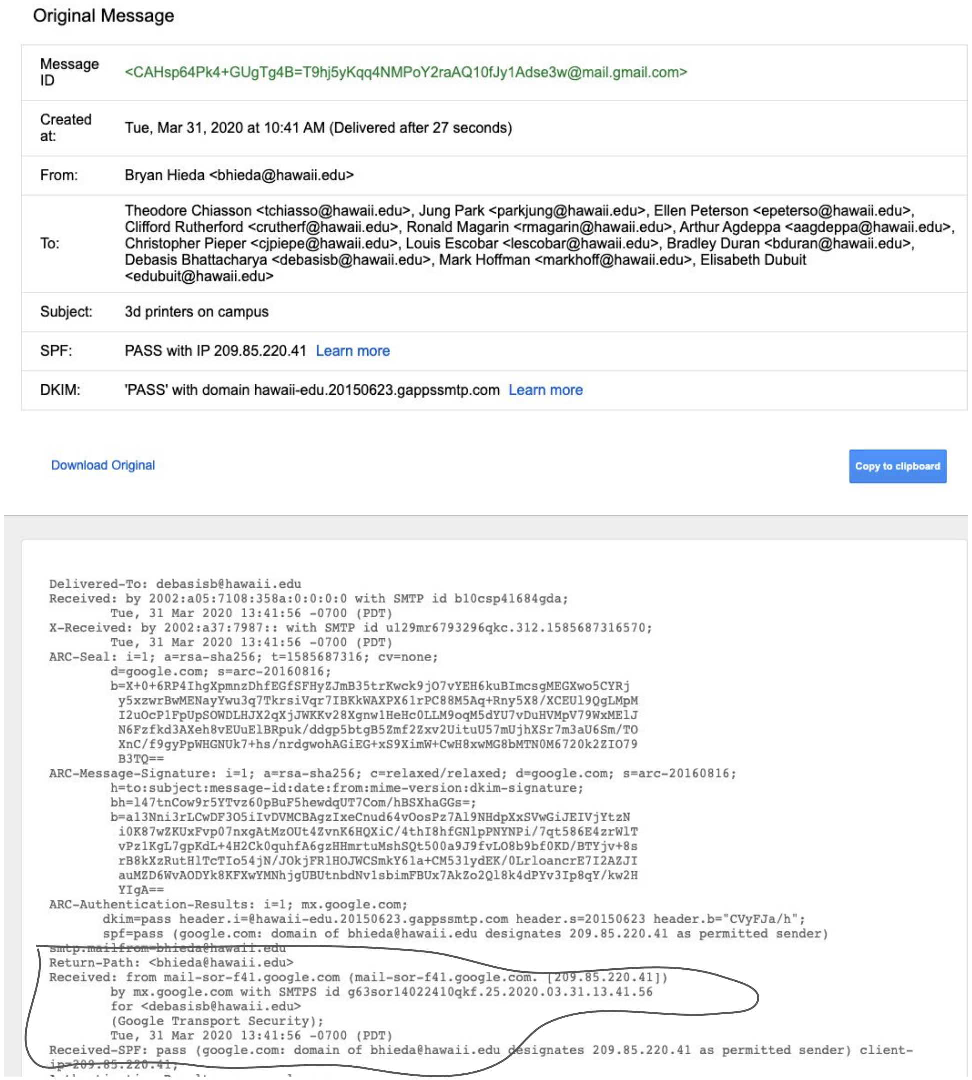
Theodore Chiasson <tchiasso@hawaii.edu> x Jung Park <parkjung@hawaii.edu> x
Ellen Peterson <epeterso@hawaii.edu> x Clifford Rutherford <crutherf@hawaii.edu> x
Ronald Magarin <rmagarin@hawaii.edu> x Arthur Aggdeppa <aagdeppa@hawaii.edu> x

Who will receive your spoofed email? Separate each recipient with a comma. You can add up to ten email addresses.

» Add CC and BCC recipients

Subject

3d printers on campus



Original Message

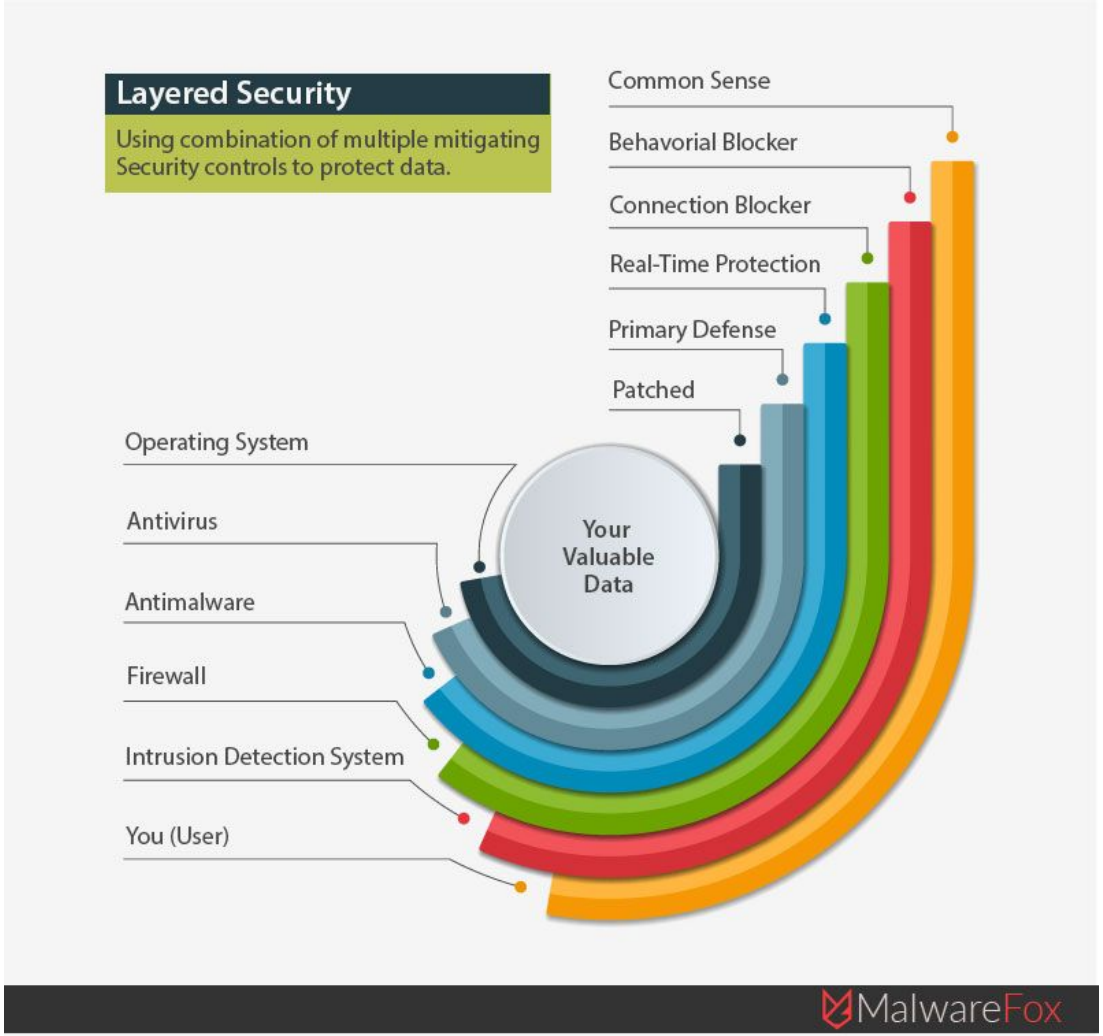
Message ID	<CAHsp64Pk4+GUgTg4B=T9hj5yKqq4NMPoY2raAQ10fJy1Adse3w@mail.gmail.com>
Created at:	Tue, Mar 31, 2020 at 10:41 AM (Delivered after 27 seconds)
From:	Bryan Hieda <bhieda@hawaii.edu>
To:	Theodore Chiasson <tchiasso@hawaii.edu>, Jung Park <parkjung@hawaii.edu>, Ellen Peterson <epeterso@hawaii.edu>, Clifford Rutherford <crutherf@hawaii.edu>, Ronald Magarin <rmagarin@hawaii.edu>, Arthur Agdeppa <aagdeppa@hawaii.edu>, Christopher Pieper <cjpiepe@hawaii.edu>, Louis Escobar <lescobar@hawaii.edu>, Bradley Duran <bduran@hawaii.edu>, Debasis Bhattacharya <debasisb@hawaii.edu>, Mark Hoffman <markhoff@hawaii.edu>, Elisabeth Dubuit <edubuit@hawaii.edu>
Subject:	3d printers on campus
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain hawaii-edu.20150623.gappssmtp.com Learn more

```
Delivered-To: debasisb@hawaii.edu
Received: by 2002:a05:7108:358a:0:0:0:0 with SMTP id b10csp41684gda;
        Tue, 31 Mar 2020 13:41:56 -0700 (PDT)
X-Received: by 2002:a37:7987:: with SMTP id u129mr6793296qkc.312.1585687316570;
        Tue, 31 Mar 2020 13:41:56 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1585687316; cv=none;
        d=google.com; s=arc-20160816;
        b=X+0+6RP4IhgXpmnzDhfEGfSFHyZJmB35trKwck9jO7vYEH6kuBImcsgMEGXwo5CYRj
         y5xzwrBwMENayYwu3q7TkrsiVqr7IBKkWAXPX61rPC88M5Aq+Rny5X8/XCEUl9QgLMpM
         I2uOcP1FpUpSOWDLHJX2qXjJWKKv28Xgnw1HeHc0LLM9oqM5dYU7vDuHVMpV79WxMElJ
         N6Fzfkd3AXeh8vEUuElBRpuk/ddgp5btgB5Zmf2Zxv2UituU57mUjhXSr7m3aU6Sm/TO
         XnC/f9gyPpWHGNUk7+hs/nrdgwohAGiEG+xS9XimW+CwH8xwMG8bMTN0M6720k2ZIO79
         B3TQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=l47tnCow9r5YTvz60pBuF5hewdqUT7Com/hBSXhaGGs=;
        b=a13Nni3rLCwDF3O5iIvDVMCBAgzIxeCnud64vOosPz7Al9NHdpXxSVwGiJEIVjYtzN
         i0K87wZKUxFvp07nxgAtMzOUt4ZvnK6HQXiC/4thI8hfGNlpPNYNPi/7qt586E4zrWlT
         vPz1KgL7gpKdL+4H2Ck0quhfA6gzHHmrtuMshSQt500a9J9fvLO8b9bf0KD/BTYjv+8s
         rB8kXzRutHlTcTIo54jN/JOkjFR1HOJWCSmkY61a+CM531ydEK/0LrloancrE7I2AZJI
         auMZD6WvAODYk8KFXwYMNhjgUBUtnbdNv1sbimFBUx7AkZo2Ql8k4dPYv3Ip8qY/kw2H
         YIgA==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@hawaii-edu.20150623.gappssmtp.com header.s=20150623 header.b="CVyFJa/h";
       spf=pass (google.com: domain of bhieda@hawaii.edu designates 209.85.220.41 as permitted sender)
smtp.mailfrom=bhieda@hawaii.edu
Return-Path: <bhieda@hawaii.edu>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id g63sor14022410qkf.25.2020.03.31.13.41.56
        for <debasisb@hawaii.edu>
        (Google Transport Security);
        Tue, 31 Mar 2020 13:41:56 -0700 (PDT)
Received-SPF: pass (google.com: domain of bhieda@hawaii.edu designates 209.85.220.41 as permitted sender) client-
ip=209.85.220.41;
```

Secure Your Home Environment

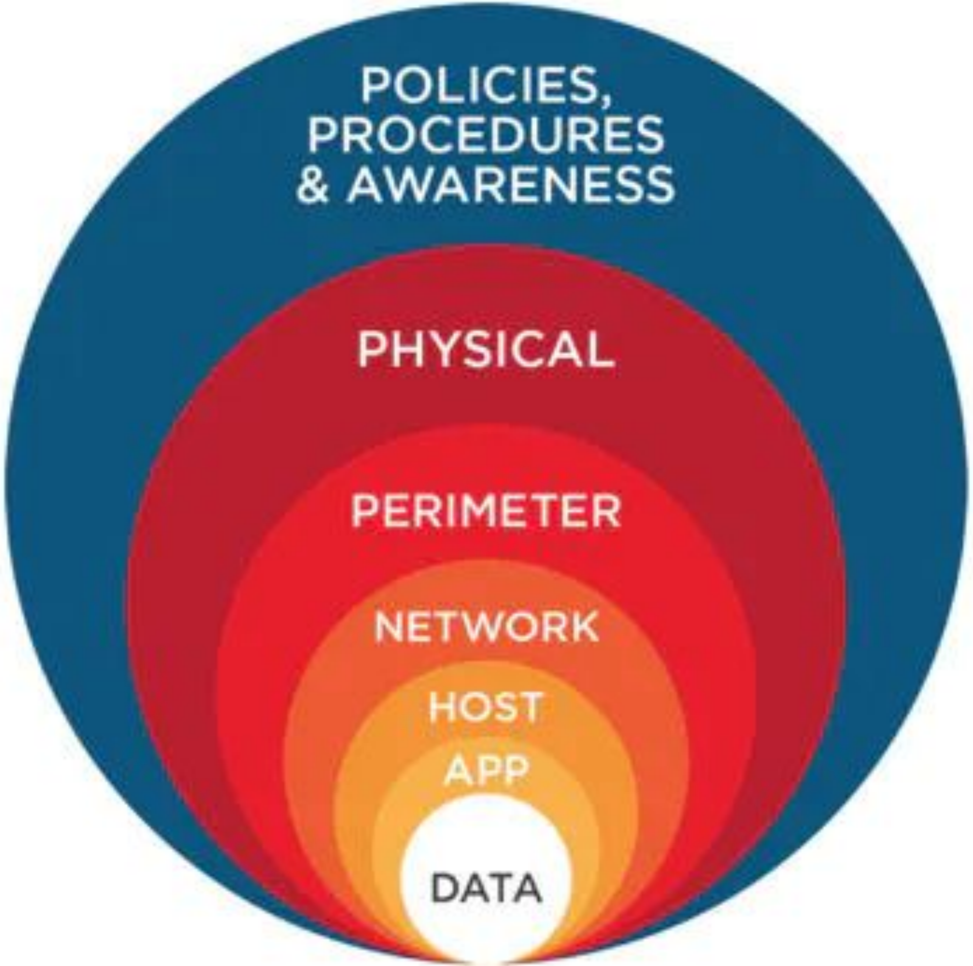
Key Concepts in Cybersecurity

- Vulnerability Analysis
  - Physical or Perimeter Security
  - Human Factors - children at home, old and vulnerable family members
  - Awareness/Expertise of Risks
  - Cost of security
  - Backup and Recovery Process
  - Business Continuity Plan
- Attack Surface
  - Total sum of vulnerabilities
  - Need to minimize the overall attack surface
- Attack Vector
  - Path or means by which an attacker can get to your computer or data
  - Humans are always the weakest link the chain
- Attack Incentives - identity, credit card, bank info, pictures, health records etc.



Layered Security

Using combination of multiple mitigating Security controls to protect data.


POLICIES,
PROCEDURES
& AWARENESS
PHYSICAL
PERIMETER
NETWORK
HOST
APP
DATA

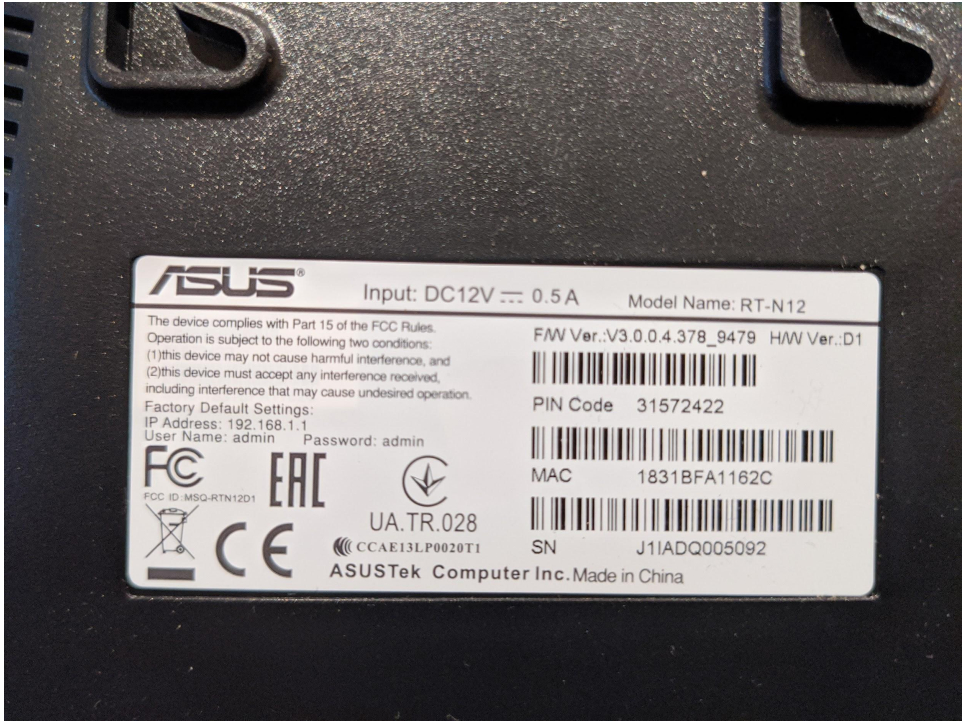
Secure Your Outer Layer - The Home Router

Home and Office Routers Are The Doorway to the Internet. How Secure Is Yours?

Think of the front door to your home. You take a variety of steps to make sure that that doorway is safe and secure from intrusion using tools like deadbolt locks and security alarms. Your router is the front door of the internet to your home or office. Are you taking the steps for the doorway of the internet into your home or office?

Routers and Websites Are Under Attack All Day, Every Day

The typical router and website will see hundreds to thousands of attempted attacks from the internet every single day. Some office websites and routers may even see attacks numbering as high as 100,000 attempted attacks in a single day. All of these attempted attacks are looking for out of date software and firmware on your router and website server so that they can get into your network and access your private information, or take over your network with malware that can be used to launch further cyber attacks against you or other potential targets.



ASUS® Input: DC12V ⎓ 0.5 A Model Name: RT-N12

The device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1)this device may not cause harmful interference, and
(2)this device must accept any interference received,
including interference that may cause undesired operation.

Factory Default Settings:
IP Address: 192.168.1.1
User Name: admin Password: admin

FCC ID:MSQ-RTN12D1

UA.TR.028

CCAE13LP0020T1

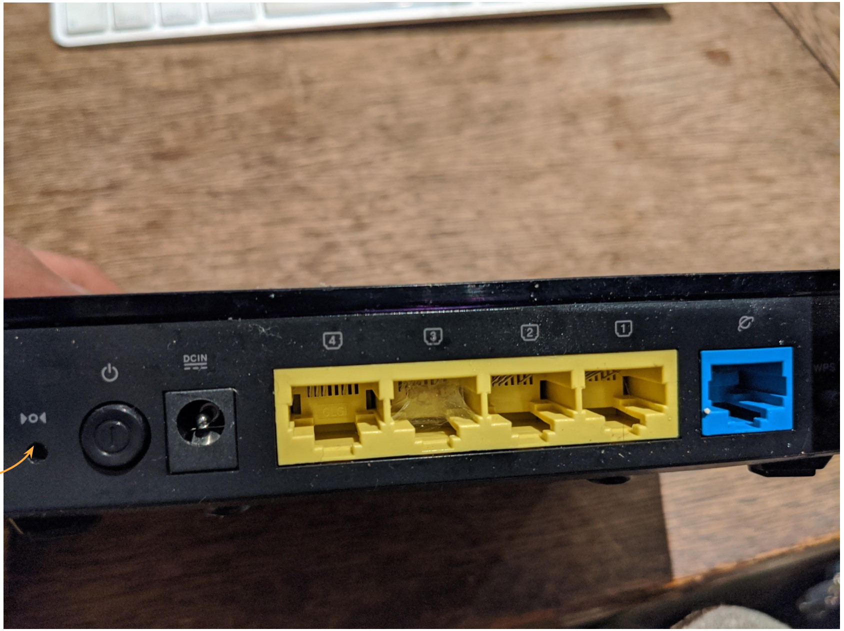
ASUSTek Computer Inc. Made in China

F/W Ver.:V3.0.0.4.378_9479 H/W Ver.:D1

PIN Code 31572422

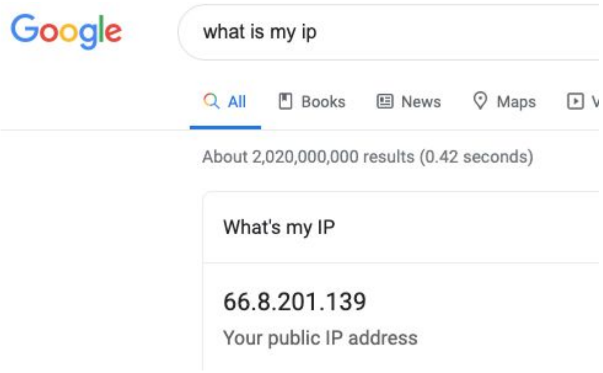
MAC 1831BFA1162C

SN J1IADQ005092



Insert a pin
to reset

ASUS RT-N12 Wireless Router
Username: admin
Password: admin

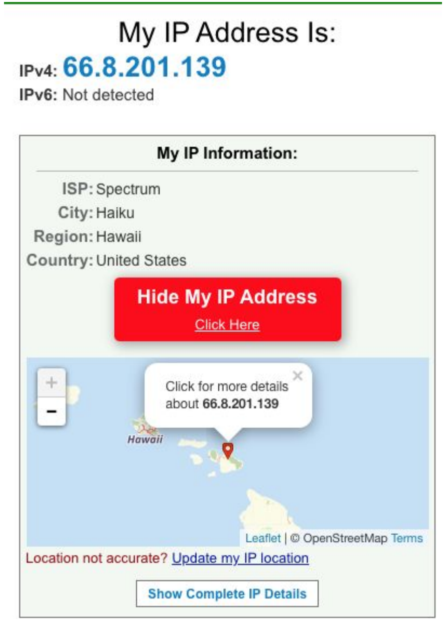


what is my ip

About 2,020,000,000 results (0.42 seconds)

What's my IP

66.8.201.139
Your public IP address



My IP Address Is:

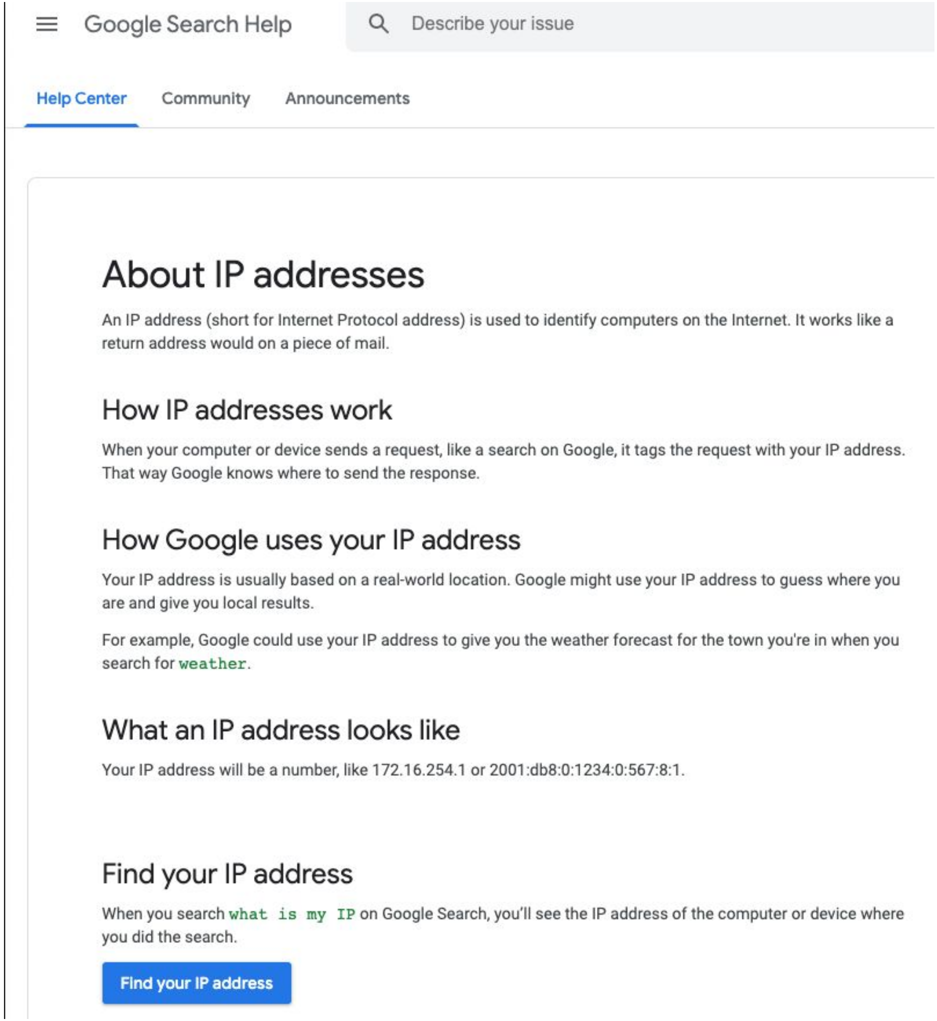
IPv4: 66.8.201.139
IPv6: Not detected

My IP Information:

ISP: Spectrum
City: Haiku
Region: Hawaii
Country: United States

Hide My IP Address
Click Here
Click for more details about 66.8.201.139
Hawaii
Leaflet | © OpenStreetMap Terms

Location not accurate? Update my IP location



About IP addresses

An IP address (short for Internet Protocol address) is used to identify computers on the Internet. It works like a return address would on a piece of mail.

How IP addresses work

When your computer or device sends a request, like a search on Google, it tags the request with your IP address. That way Google knows where to send the response.

How Google uses your IP address

Your IP address is usually based on a real-world location. Google might use your IP address to guess where you are and give you local results.

For example, Google could use your IP address to give you the weather forecast for the town you're in when you search for `weather`.

What an IP address looks like

Your IP address will be a number, like 172.16.254.1 or 2001:db8:0:1234:0:567:8:1.

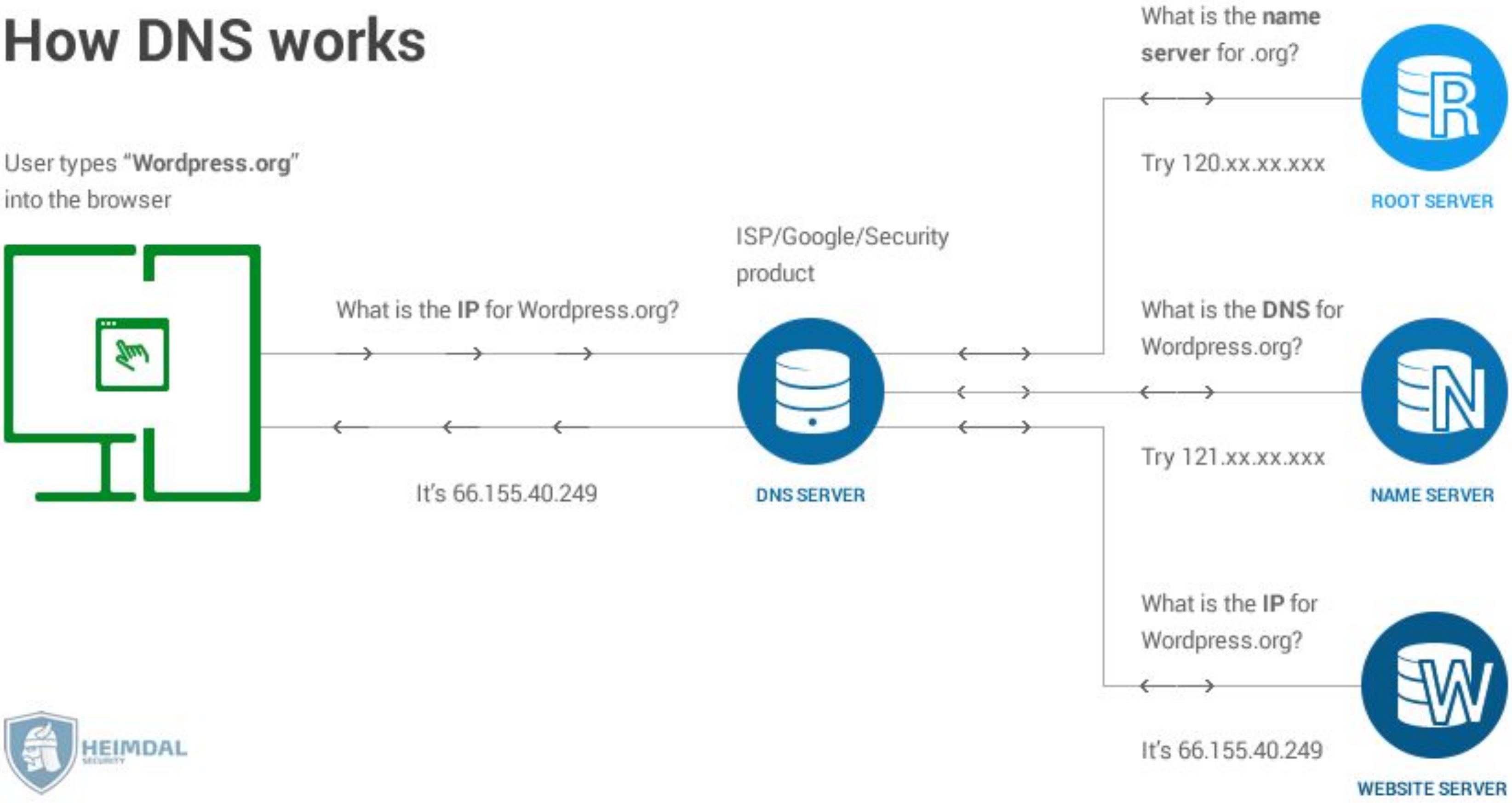
Find your IP address

When you search `what is my IP` on Google Search, you'll see the IP address of the computer or device where you did the search.

Basic Steps to Secure your Wi-Fi Home Router

- Access the Router Screen
  - http://192.168.0.1 or
  - http://192.168.1.1
- Change the Default Password to a Strong Password
- Setup WPA2 security for Wi-Fi access
- Keep the Firmware Updated
- Disable Remote Access, UPnP and WPS
- Use a Guest Network, only if needed
- Note that home router connects many endpoints
  - Computers, cell phones, game consoles, printers, security cameras, other IoT sensors
- Home network usually has both Wi-Fi and Wired connections
- Source: https://www.wired.com/story/secure-your-wi-fi-router/

How DNS works



User types “**Wordpress.org**” into the browser

What is the **IP** for Wordpress.org?

It’s 66.155.40.249

ISP/Google/Security product

What is the **name server** for .org?

Try 120.xx.xx.xxx

What is the **DNS** for Wordpress.org?

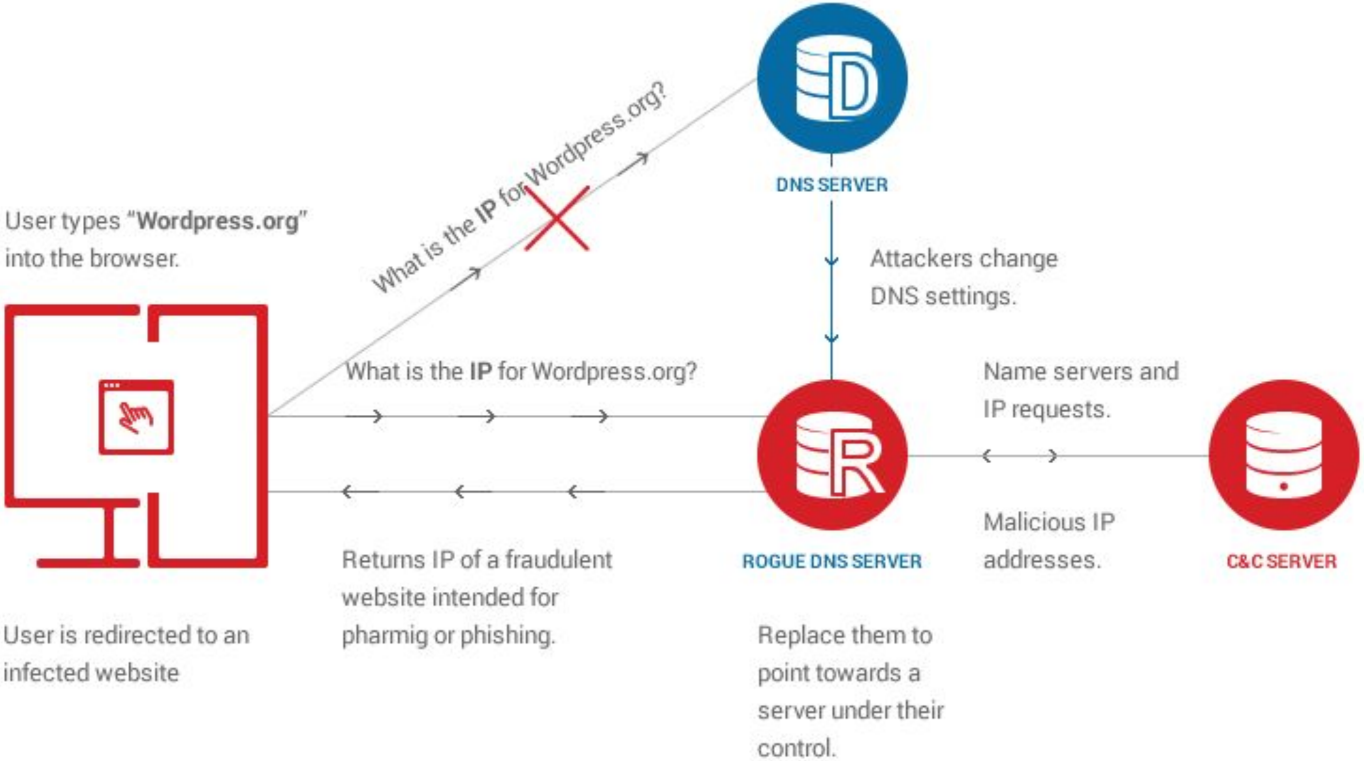
Try 121.xx.xx.xxx

What is the **IP** for Wordpress.org?

It’s 66.155.40.249

HEIMDAL SECURITY

DNS Hijacking attack



User types "**Wordpress.org**" into the browser.

What is the **IP** for Wordpress.org?

DNS SERVER

Attackers change DNS settings.

What is the **IP** for Wordpress.org?

Name servers and IP requests.

Malicious IP addresses.

ROGUE DNS SERVER

C&C SERVER

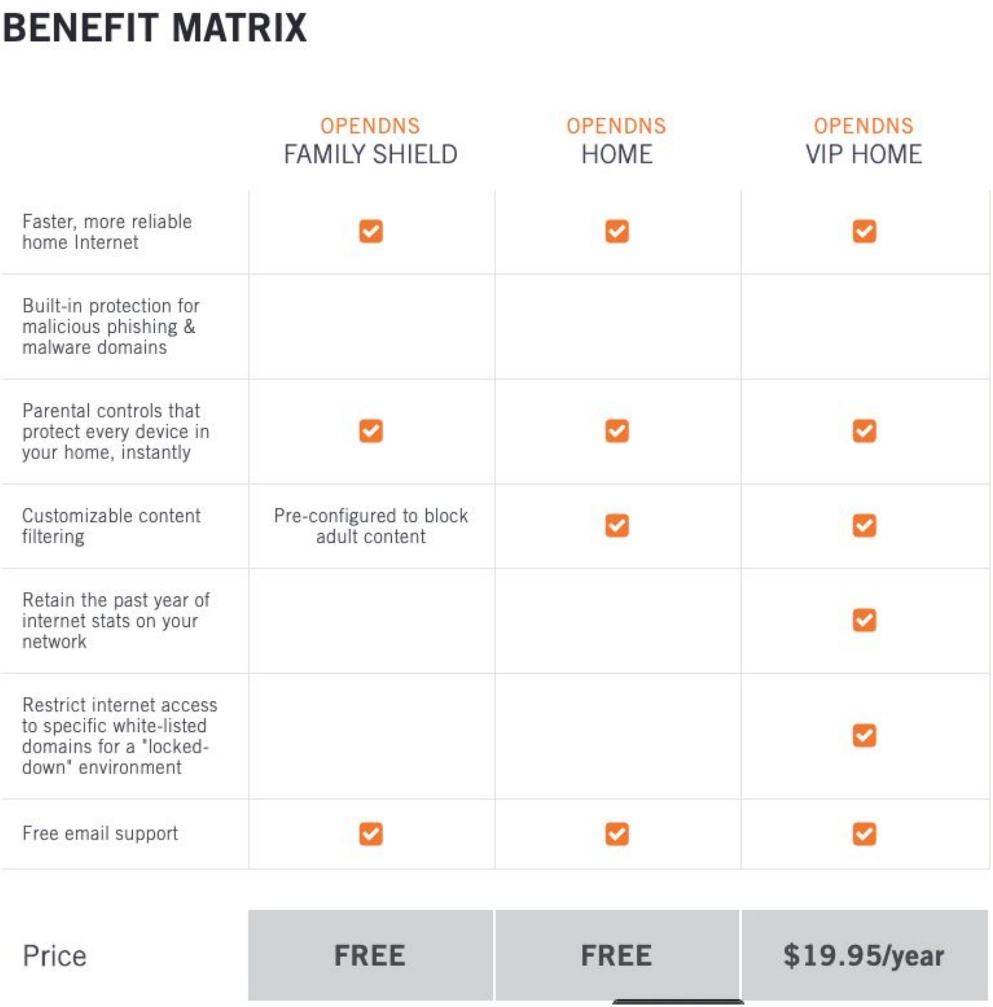
Returns IP of a fraudulent website intended for pharmig or phishing.

User is redirected to an infected website

Replace them to point towards a server under their control.

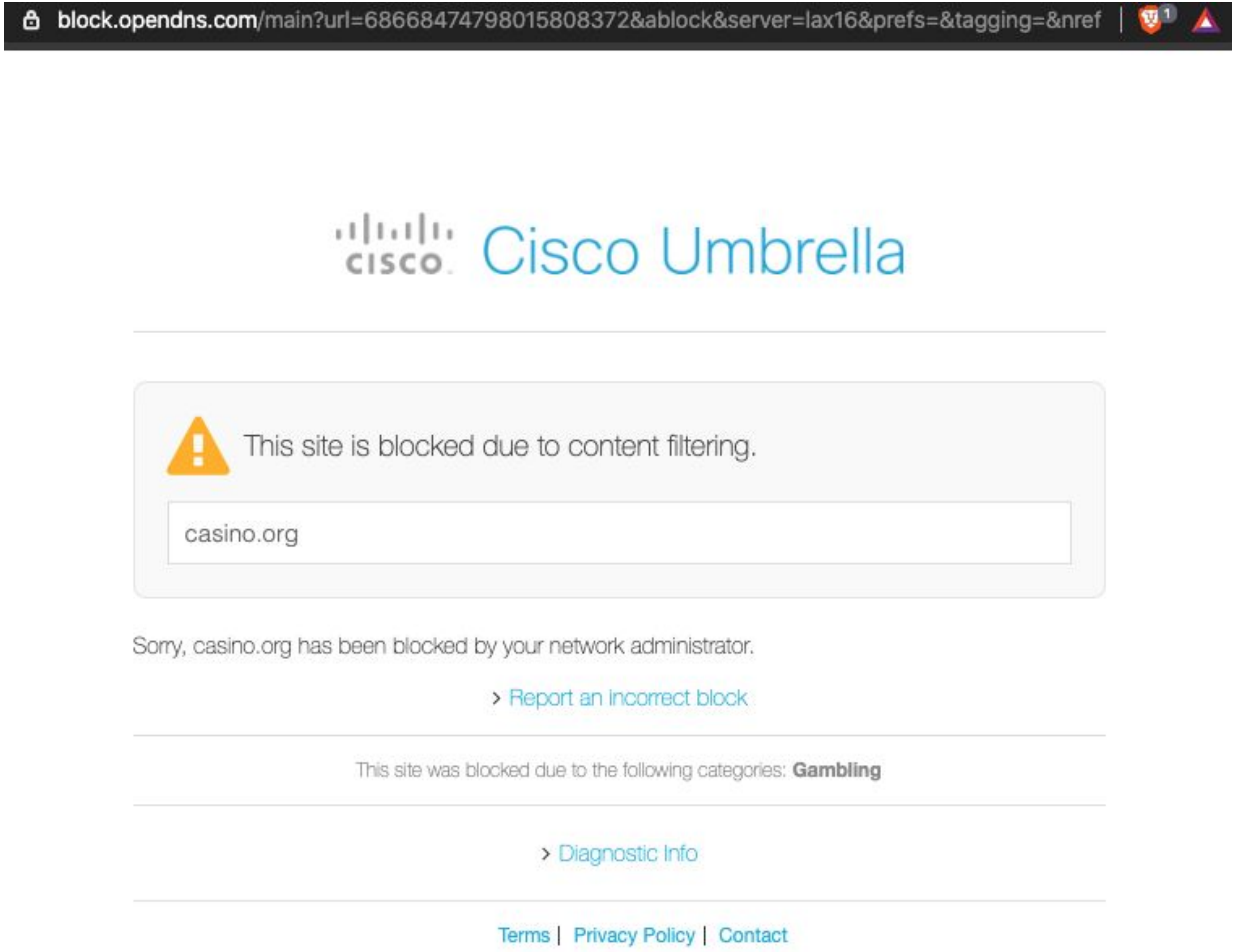
opendns.com/home-internet-security/
cisco
OpenDNS is now part of Cisco
OpenDNS
CONSUMER
OpenDNS Packages | What They Are Saying |

OPENDNS SETTINGS APPLY TO EVERY DEVICE — laptops, smartphones, tablets, DVRs, game consoles, TVs, literally anything that connects to the internet from your home network. Not to mention, we're one of the world's leading DNS service providers, meaning you'll experience faster internet speeds as well. Reliable & fast – what's better than that?



BENEFIT MATRIX

	OPENDNS FAMILY SHIELD	OPENDNS HOME	OPENDNS VIP HOME
Faster, more reliable home Internet	☑	☑	☑
Built-in protection for malicious phishing & malware domains			
Parental controls that protect every device in your home, instantly	☑	☑	☑
Customizable content filtering	Pre-configured to block adult content	☑	☑
Retain the past year of internet stats on your network			☑
Restrict internet access to specific white-listed domains for a "locked-down" environment			☑
Free email support	☑	☑	☑
Price	FREE	FREE	$19.95/year



block.opendns.com/main?url=68668474798015808372&ablock&server=lax16&prefs=&tagging=&nref

Cisco Umbrella

This site is blocked due to content filtering.

casino.org

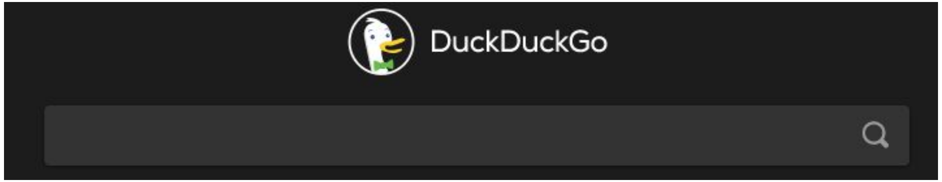
Sorry, casino.org has been blocked by your network administrator.

› Report an incorrect block

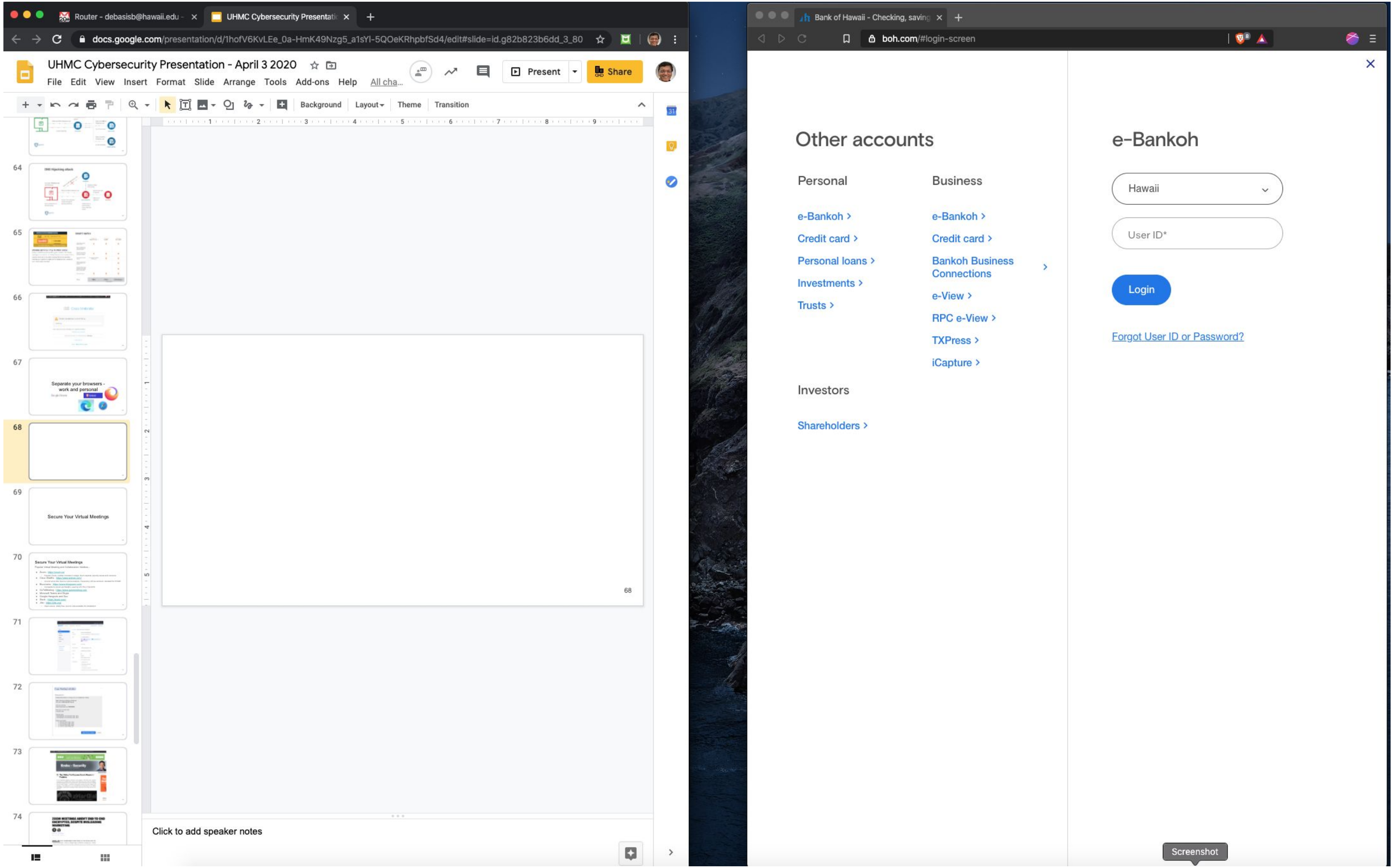
This site was blocked due to the following categories: **Gambling**

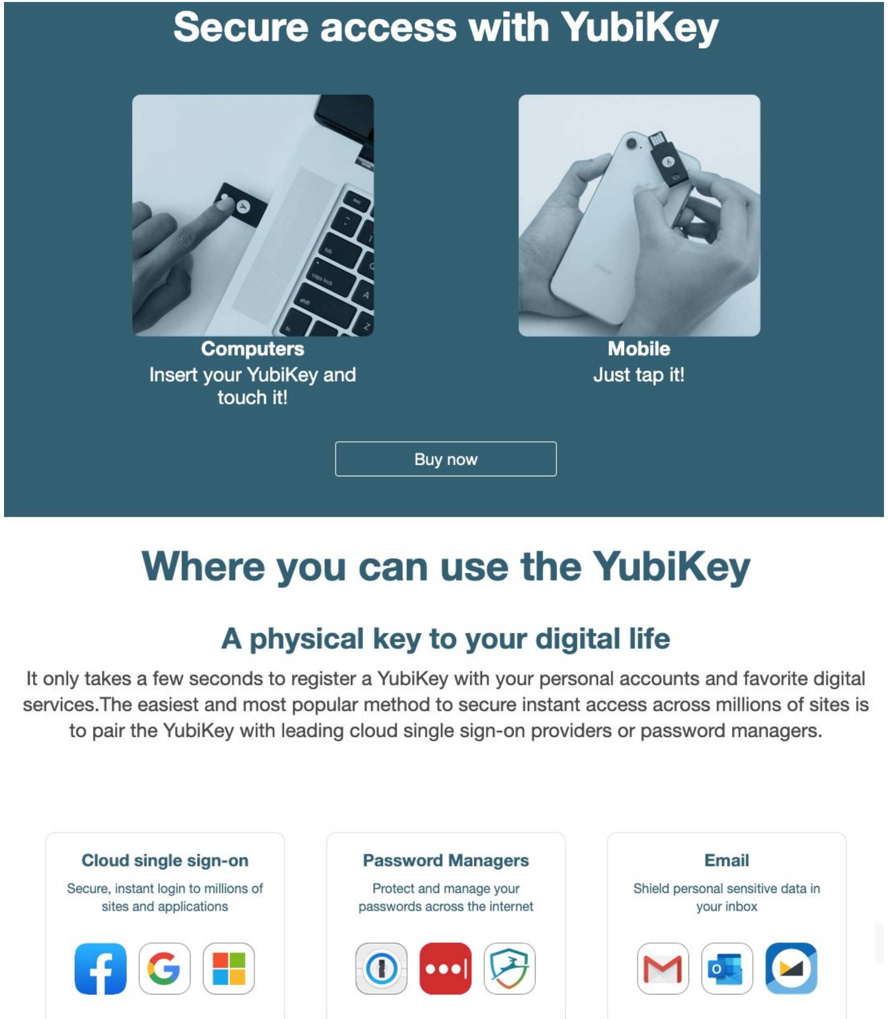
› Diagnostic Info

Terms | Privacy Policy | Contact



Separate search engine and browsers - work and personal


Router - debasisb@hawaii.edu
UHMC Cybersecurity Presentation
docs.google.com/presentation/d/1hofV6KvLEe_0a-HmK49Nzg5_a1sYl-5QOeKRhpbfSd4/edit#slide=id.g82b823b6dd_3_80
UHMC Cybersecurity Presentation - April 3 2020
File Edit View Insert Format Slide Arrange Tools Add-ons Help All cha...
Present
Share
Background
Layout
Theme
Transition
Separate your browsers - work and personal
Secure Your Virtual Meetings
68
Click to add speaker notes
Bank of Hawaii - Checking, saving
boh.com/#login-screen
Other accounts
Personal
e-Bankoh ›
Credit card ›
Personal loans ›
Investments ›
Trusts ›
Business
e-Bankoh ›
Credit card ›
Bankoh Business Connections ›
e-View ›
RPC e-View ›
TXPress ›
iCapture ›
Investors
Shareholders ›
e-Bankoh
Hawaii
User ID*
Login
Forgot User ID or Password?
Screenshot



Secure access with YubiKey

Computers
Insert your YubiKey and touch it!

Mobile
Just tap it!

Where you can use the YubiKey

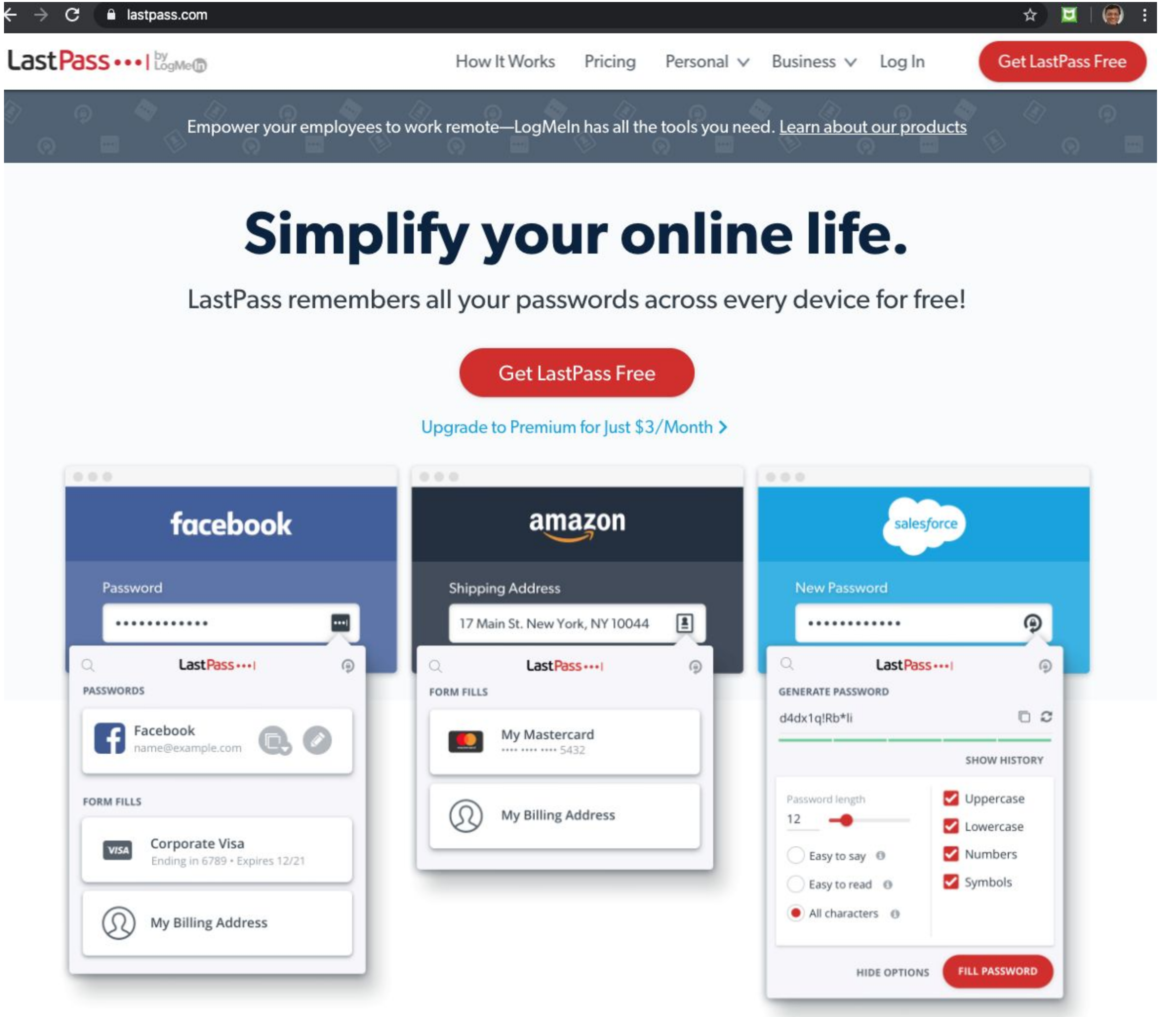
A physical key to your digital life

It only takes a few seconds to register a YubiKey with your personal accounts and favorite digital services.The easiest and most popular method to secure instant access across millions of sites is to pair the YubiKey with leading cloud single sign-on providers or password managers.

Cloud single sign-on
Secure, instant login to millions of sites and applications

Password Managers
Protect and manage your passwords across the internet

Email
Shield personal sensitive data in your inbox



Empower your employees to work remote—LogMeIn has all the tools you need. Learn about our products

Simplify your online life.

LastPass remembers all your passwords across every device for free!

Children and family members at home

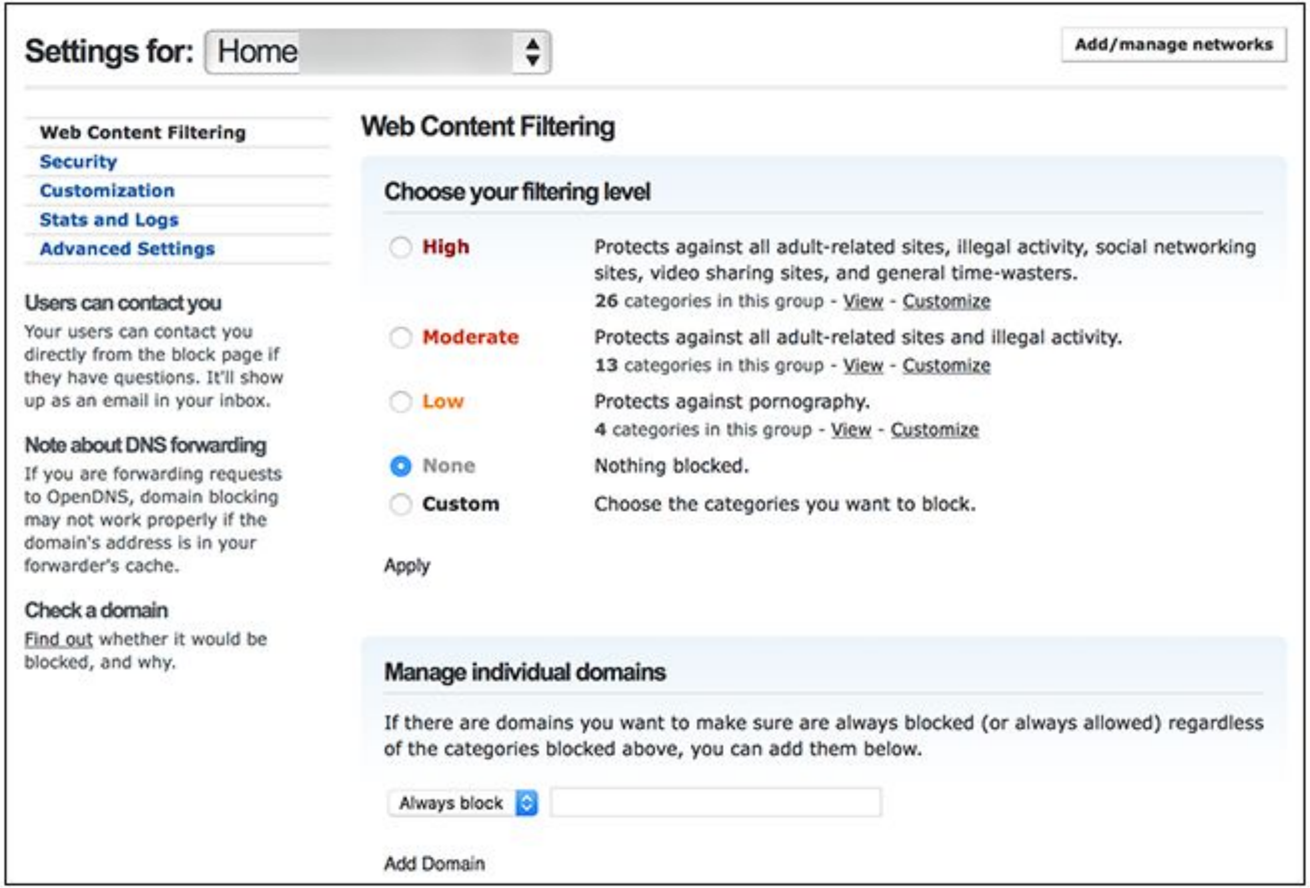
Vulnerability Assessment needs to include children and family members

Increases the Attack Surface and adds Attack Vectors

  - Use Virtual Private Networks (VPNs) to online content
  - Access social media tools
  - Targeted by spam, online harassment, predators etc.
  - Could download malware, botnets, ransomware etc.
  - Internet access is available via cell data connections, as well as through home router

- Decrease Attack Surface by Layered Security
  - Keeping work computer separate from home computer
  - Perimeter security - keep the work area safe and secure
  - Keep work cell phone safe and separate from home users
  - Lock screen of cell phones, auto lock computer screen, shutdown work computers

opendns.com/home-internet-security/
CISCO
OpenDNS is now part of Cisco
OpenDNS
CONSUMER
OpenDNS Packages
What They Are Saying



Settings for: Home

Web Content Filtering

Choose your filtering level

○ **High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.
26 categories in this group - View - Customize

○ **Moderate** Protects against all adult-related sites and illegal activity.
13 categories in this group - View - Customize

○ **Low** Protects against pornography.
4 categories in this group - View - Customize

● None Nothing blocked.

○ **Custom** Choose the categories you want to block.

Apply

Manage individual domains

If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

Always block

Add Domain

Users can contact you

Your users can contact you directly from the block page if they have questions. It'll show up as an email in your inbox.

Note about DNS forwarding

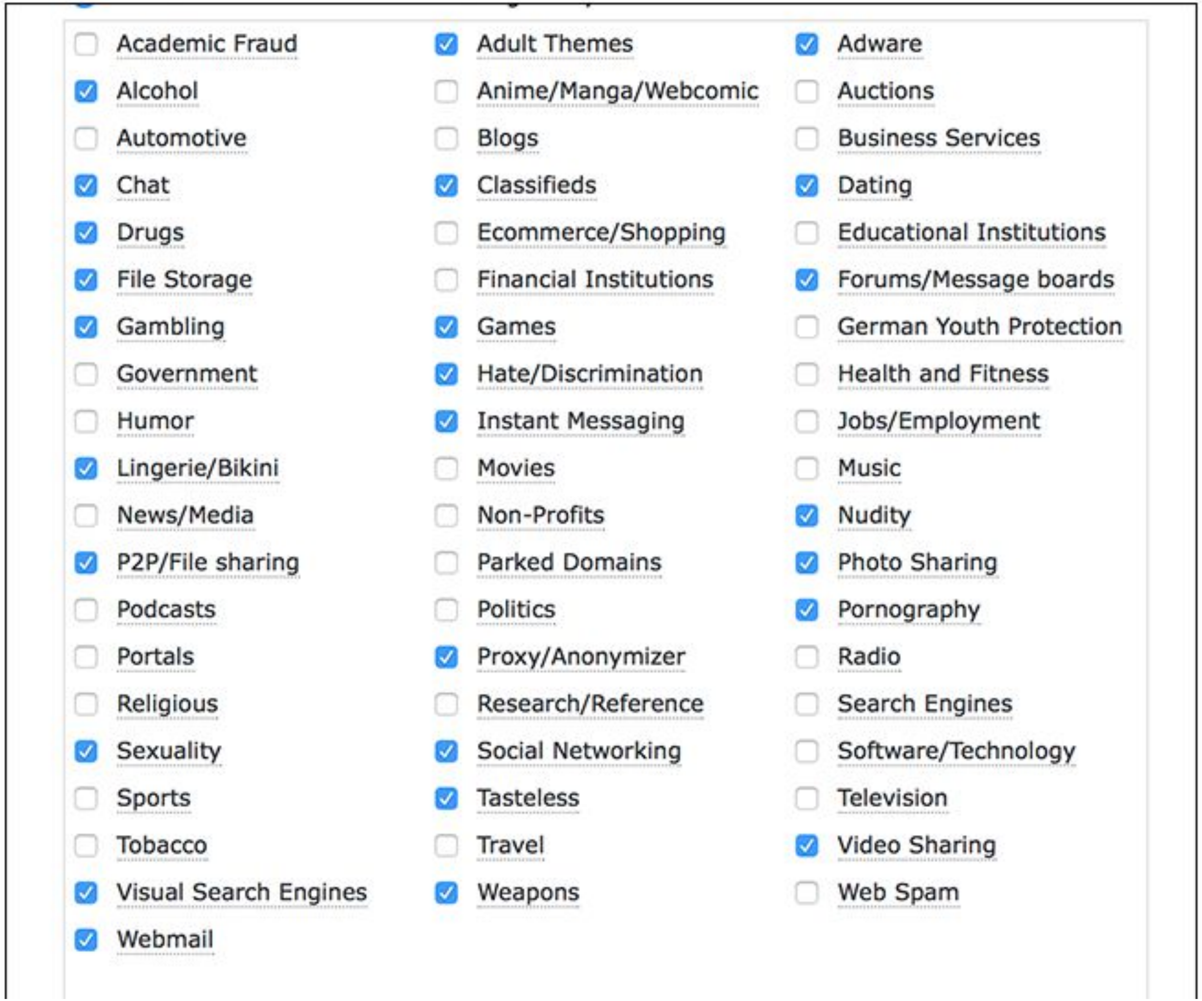
If you are forwarding requests to OpenDNS, domain blocking may not work properly if the domain's address is in your forwarder's cache.

Check a domain

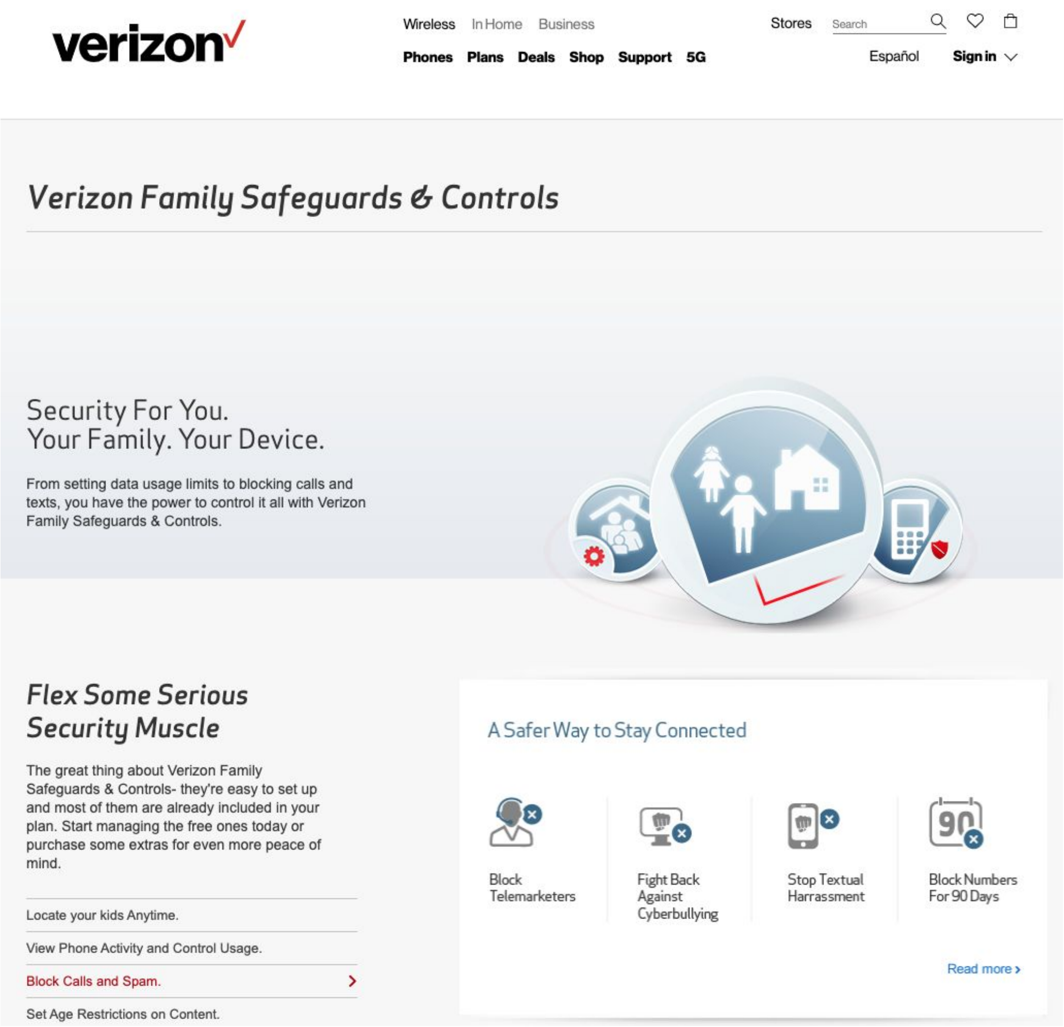
Find out whether it would be blocked, and why.

opendns.com/home-internet-security/
CISCO
OpenDNS is now part of Cisco
OpenDNS
CONSUMER
OpenDNS Packages
What They Are Saying

Source OpenDNS: https://www.howtogeek.com/79998/protect-your-kids-online-using-open-dns-2/



- □ Academic Fraud
- ☑ Adult Themes
- ☑ Adware
- ☑ Alcohol
- □ Anime/Manga/Webcomic
- □ Auctions
- □ Automotive
- □ Blogs
- □ Business Services
- ☑ Chat
- ☑ Classifieds
- ☑ Dating
- ☑ Drugs
- □ Ecommerce/Shopping
- □ Educational Institutions
- ☑ File Storage
- □ Financial Institutions
- ☑ Forums/Message boards
- ☑ Gambling
- ☑ Games
- □ German Youth Protection
- □ Government
- ☑ Hate/Discrimination
- □ Health and Fitness
- □ Humor
- ☑ Instant Messaging
- □ Jobs/Employment
- ☑ Lingerie/Bikini
- □ Movies
- □ Music
- □ News/Media
- □ Non-Profits
- ☑ Nudity
- ☑ P2P/File sharing
- □ Parked Domains
- ☑ Photo Sharing
- □ Podcasts
- □ Politics
- ☑ Pornography
- □ Portals
- ☑ Proxy/Anonymizer
- □ Radio
- □ Religious
- □ Research/Reference
- □ Search Engines
- ☑ Sexuality
- ☑ Social Networking
- □ Software/Technology
- □ Sports
- ☑ Tasteless
- □ Television
- □ Tobacco
- □ Travel
- ☑ Video Sharing
- ☑ Visual Search Engines
- ☑ Weapons
- □ Web Spam
- ☑ Webmail



Verizon Family Safeguards & Controls

Security For You.
Your Family. Your Device.

From setting data usage limits to blocking calls and texts, you have the power to control it all with Verizon Family Safeguards & Controls.

Flex Some Serious Security Muscle

The great thing about Verizon Family Safeguards & Controls- they're easy to set up and most of them are already included in your plan. Start managing the free ones today or purchase some extras for even more peace of mind.

Locate your kids Anytime.

View Phone Activity and Control Usage.

Block Calls and Spam.

Set Age Restrictions on Content.

A Safer Way to Stay Connected

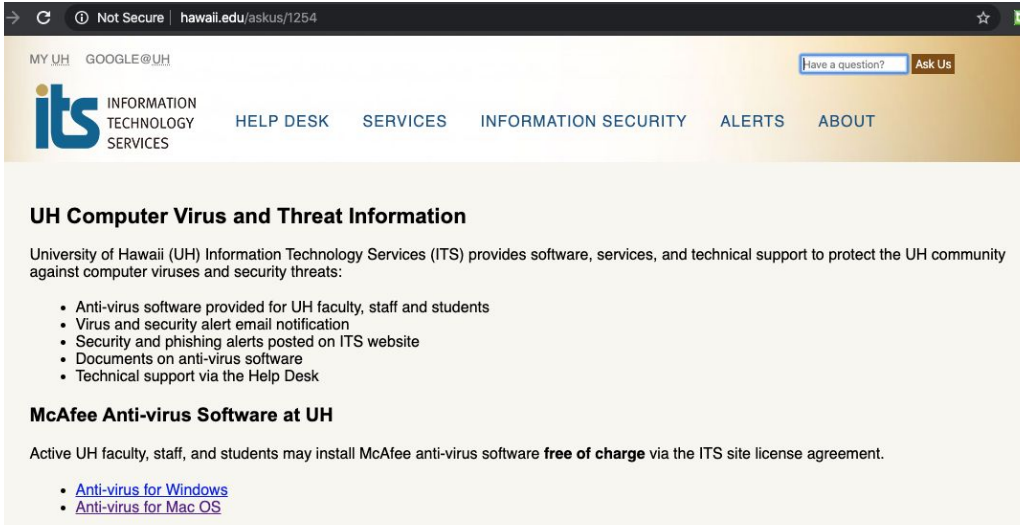
Block Telemarketers

Fight Back Against Cyberbullying

Stop Textual Harrassment

Block Numbers For 90 Days

Read more ›



UH Computer Virus and Threat Information

University of Hawaii (UH) Information Technology Services (ITS) provides software, services, and technical support to protect the UH community against computer viruses and security threats:

- Anti-virus software provided for UH faculty, staff and students
- Virus and security alert email notification
- Security and phishing alerts posted on ITS website
- Documents on anti-virus software
- Technical support via the Help Desk

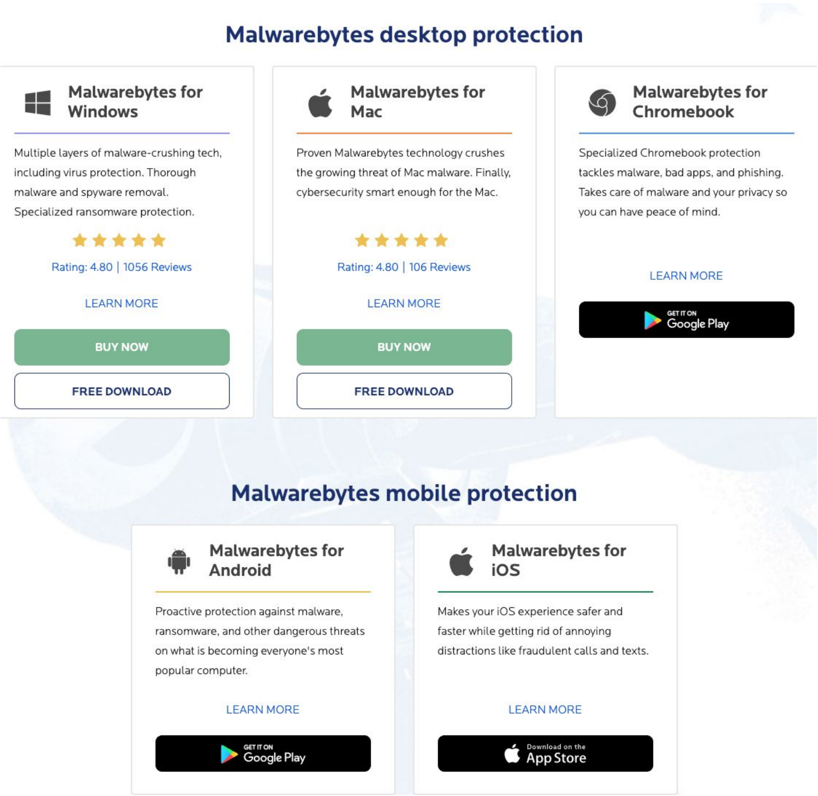
McAfee Anti-virus Software at UH

Active UH faculty, staff, and students may install McAfee anti-virus software **free of charge** via the ITS site license agreement.

- Anti-virus for Windows
- Anti-virus for Mac OS

Work Computers

Home Computers and Cell Phones



Malwarebytes desktop protection

Malwarebytes for Windows

Multiple layers of malware-crushing tech, including virus protection. Thorough malware and spyware removal. Specialized ransomware protection.

★★★★★

Rating: 4.80 | 1056 Reviews

Malwarebytes for Mac

Proven Malwarebytes technology crushes the growing threat of Mac malware. Finally, cybersecurity smart enough for the Mac.

★★★★★

Rating: 4.80 | 106 Reviews

Malwarebytes for Chromebook

Specialized Chromebook protection tackles malware, bad apps, and phishing. Takes care of malware and your privacy so you can have peace of mind.

Malwarebytes mobile protection

Malwarebytes for Android

Proactive protection against malware, ransomware, and other dangerous threats on what is becoming everyone's most popular computer.

Malwarebytes for iOS

Makes your iOS experience safer and faster while getting rid of annoying distractions like fraudulent calls and texts.

Secure Your Virtual Meetings

Secure Your Virtual Meetings

Popular Virtual Meeting and Collaboration Vendors -

- Zoom - https://zoom.us/
  - Popular choice, sudden increase in usage, Zoom exploits, security issues and concerns
- Cisco WebEx - https://www.webex.com/
  - Around since 90s. Secure communications. Favored by US Government, standard for HI DoE
- BlueJeans - https://www.bluejeans.com/
- GoToMeeting - https://www.gotomeeting.com
- RingCentral - https://www.ringcentral.com
- Microsoft Teams in Microsoft 365 (formerly Office 365) and Skype
- Google Meet (new, formerly Hangouts and Duo) - https://meet.google.com/
- Slack - https://slack.com/
- Jitsi - https://jitsi.org/
  - Open source, totally free, source code available for installation!

Key Principles for Securing Virtual Meetings

1. Publicizing the meeting
    a. Need to know - Only your meeting participants need to know about your meeting URL
    b. Separate publicity of URL with a private message about unique meeting password
2. Joining the meeting
    a. By Invitation - have a Auto Generated Link and Require Unique Password
    b. By Time - meeting does not start without the host present
    c. Access Privilege - usually a sign-on login, waiting room to screen and admit participants
    d. Identity - display a login name or show up on video (ask and verify all audio/phone calls)
    e. Authentication - verify that person is who they claim to be (need to check all phone callers)
3. Conducting the meeting
    a. Host controls who shares the screen. Make others a co-host only when necessary
    b. Host controls all video, audio, whiteboard, annotations and chat privileges of participants
    c. Host locks meeting after start and can expel participant(s) without warning
4. Storage and distribution of meeting recording
    a. Host stores, creates closed captions and distributes recording of meeting in a secure manner!

HI DoE Security Guidance

Jonathan Chee

Using Google Securely

- Verify Google Add-ons, Extensions, Third-Party Applications
    - Read the Privacy Notices
    - Will student data be captured and stored? If yes where and how is it being secured?
    - What security measures do they have in place?
- Use Shared Drives instead of emailing documents
    - Only works with Google accounts

- Share documents with specific people instead of using “anyone with the link”

- Limit the use of shared accounts

Limit Public Information and Exposure

- Posting personal information on Social media sites
    - Linkedin
    - Facebook
- Do not post Staff email addresses on your school websites
    - Use contact forms or messaging systems built into your websites
- Be cognizant of the websites you signup for and the passwords you use
    - Compromised websites provide easy information
    - https://haveibeenpwned.com/

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

INFORMATION
TECHNOLOGY
SERVICES

Q&A, Comments, Feedback!

Debasis Bhattacharya (debasisb@hawaii.edu)
Jonathan Chee (Jonathan.Chee@k12.hi.us)

Presentation Available @ maui.hawaii.edu/cybersecurity