COVID-19 Scams

*Webinar will begin promptly at 2pm Eastern

*Webinar is being recorded

www.staysafeonline.org

@staysafeonline
✓ **Convening** partners who recognize strength in the security collective

✓ **Educating** individuals & organizations on cybersecurity best practices

✓ **Amplifying** collective efforts to increase cybersecurity awareness

[www.staysafeonline.org](http://www.staysafeonline.org)  @staysafeonline
Thanks to our National Sponsors

Signature Sponsor

TREND MICRO

education

Affiliate Sponsor

GENERALI GLOBAL ASSISTANCE
IDENTITY PROTECTION SERVICES

Strategic Partner

ITSP MAGAZINE

All the intersection of IT Security & Society

“This was an excellent webinar with good information for small businesses and tech support companies like us who provide advice on support and security to our customers. The information covered can be passed along to our customers so they are #CyberAware!"
Today’s Guest Speakers

Lesley Fair
Senior Attorney
Bureau of Consumer Protection
Federal Trade Commission

Jon Clay
Cybersecurity Expert and
Director of Global Threat Communications
Trend Micro

William Malik
Vice President, Infrastructure Strategies
Trend Micro

Patrice Bobola
Head of Global IDP Knowledge & QA
Generali Global Assistance

(MODERATOR)
Daniel Eliot
Director of Education & Strategic Initiatives
National Cyber Security Alliance

*This webinar will be recorded and will be distributed to registrants after the webinar concludes*
THE COVID-19 CRISIS
and the FTC’s consumer protection response

Lesley Fair
Senior Attorney
Bureau of Consumer Protection
Federal Trade Commission
The FTC’s Response

- Analyze reports from consumers.
- Warn companies engaging in possible illegal conduct.
- Educate consumers and businesses about how to protect themselves.
- Bring law enforcement actions.
# FTC COVID-19 Complaints

**January 1, 2020 - April 30, 2020**

<table>
<thead>
<tr>
<th>Category</th>
<th>Reports</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>17,889</td>
<td>$21,97M</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>2,401</td>
<td></td>
</tr>
<tr>
<td>Do Not Call</td>
<td>1,751</td>
<td>$532</td>
</tr>
</tbody>
</table>

*44.2% of fraud complaints report a loss

## Top Fraud Products or Services (Top 5 by # of Reports and $ Loss)

<table>
<thead>
<tr>
<th>Service</th>
<th>Reports</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Travel/Vacations</td>
<td>4,784</td>
<td>$8,041K</td>
</tr>
<tr>
<td>Online Shopping</td>
<td>3,358</td>
<td>$2,196K</td>
</tr>
<tr>
<td>Mobile: Text Messages</td>
<td>1,368</td>
<td>$167K</td>
</tr>
<tr>
<td>Internet Information Services</td>
<td>665</td>
<td>$338K</td>
</tr>
<tr>
<td>Imposter: Business</td>
<td>617</td>
<td>$1,614K</td>
</tr>
</tbody>
</table>

*While the travel/vacation category typically relates to the sale or advertising of these services, the Coronavirus-related complaints in this category are primarily about refunds and cancellations.*
... often perpetrated via robocall
WARNING LETTER

Date: March 26, 2020

TO: info@corona-cure.com
    corona-cure.com@domainsbyproxy.com

RE: Unapproved and Misbranded Products Related to Coronavirus Disease 2019 (COVID-19)

This is to advise you that the United States Food and Drug Administration (FDA) and the Federal Trade Commission (FTC) reviewed your website at the Internet address https://corona-cure.com in March 2020. The FDA has determined that your website offers Corona-Cure Coronavirus Infection Prevention Nasal Spray for sale in the United States and that this product is intended to mitigate, prevent, treat, diagnose, or cure COVID-19 in people. FDA has determined that this product is an unapproved new drug sold in violation of section 505(a) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. § 355(a). Furthermore, this product is a misbranded drug under section 502 of the FD&C Act, 21 U.S.C. § 352. The introduction or delivery for introduction of this product into interstate commerce is prohibited under sections 301(a) and (d) of the FD&C Act, 21 U.S.C. § 331(a) and (d).
NOTE: This page contains a sample letter to VoIP companies facilitating robocalls. The full content is provided in the raw text below.

WARNING LETTERS TO VoIP COMPANIES FACILITATING ROBOCALLS

April 3, 2020

VIA CERTIFIED MAIL - RETURN RECEIPT REQUESTED AND EMAIL

To: Chris Cordero
Connexum
1122 E. Lincoln Ave.
Suite 203
Orange, CA 92865
cordero@connexum.com

Scott Kettle
Connexum
17901 Von Karman Ave.
Suite 600
Irvine, CA 92614
sk@connexumllc.com

Re: Official Correspondence from Federal Communications Commission and Federal Trade Commission

Dear Mssrs. Cordero and Kettle,

We have determined that Connexum is apparently routing and transmitting Novel Coronavirus Disease (COVID-19) scam robocall traffic originating from VoIPMax. We request that you cease routing and transmitting such traffic immediately.
Accordingly, if after 48 hours of the release of this letter, any of the above-listed gateway or originating provider(s) continues to route or transmit the above named originators’ robocalls on its network—in other words, if it continues to facilitate the entry of unlawful robocalls onto American networks—the FCC will: (1) authorize other U.S. providers to block all calls coming from that gateway or originating provider; and (2) authorize other U.S. providers to take any other steps as needed to prevent further transmission of unlawful calls originating from the originator(s) listed above. The FCC will also authorize U.S. providers to extend the obligation to prevent transmission of these unlawful calls with all entities with which they contract or that handle traffic in any part of the call path.

TRANSLATION: DONTCHABE
The Federal Trade Commission continues its work protecting consumers, providing guidance to businesses, and protecting competition in the marketplace throughout the pandemic. Staff are working remotely and events that are not postponed are being held via webcast.

**FOR CONSUMERS**
Helping people spot and avoid the latest Coronavirus scams.

*More for consumers >*

**FOR BUSINESSES**
Offering compliance guidance for companies and tips on protecting against scams targeting businesses.

*More for business >*

**ENFORCEMENT**
Updating the public on FTC law enforcement actions and complaint data.

*More on enforcement >*
CORONAVIRUS RESOURCES
for consumers

KEEP CALM and Avoid Coronavirus Scams

Here are 5 things you can do to avoid a Coronavirus scam:

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

Hang up on robocalls. Scammers use illegal sales call to get your money and your personal information.

Watch out for phishing emails and text messages. Don’t click on links in emails or texts you didn’t expect.

Research before you donate. Don’t let anyone rush you into making a donation. Get tips on donating wisely at ftc.gov/charity.

Stay in the know. Go to ftc.gov/pressroom and ftc.gov/coronavirus for the latest information on scams. Sign up to get FTC’s alerts at ftc.gov/alerts.

Scam Alerts

- Avoid scams while finding help during quarantine
- While you’re at home, spot the scams
- 60 and over in the time of COVID-19? Read on
- Thinking critically about Coronavirus news and information
- Now more than ever, spot the scams with #FTCScamBingo
- FTC: Coronavirus scams, Part 2
- Coronavirus: Scammers follow the headlines

FINANCIAL IMPACT of the Coronavirus
CORONAVIRUS RESOURCES for business

Seven Coronavirus scams targeting your business

By: Lesley Fair | Mar 25, 2020 | 1:30PM

We’ve warned consumers about Coronavirus-related scams, but businesses are at risk, too. Keep your guard up against these seven B2B scams that try to exploit companies’ concerns about COVID-19. In addition to sharing this information with your employees and social networks, read on for how you can report Coronavirus scams to the FTC.

PUBLIC HEALTH SCAMS
Fraudsters are sending messages that claim to be from the Centers for Disease Control and Prevention (CDC), World Health Organization (WHO), or other public health offices. They may ask for Social Security numbers, tax IDs, etc. Other variations direct you to click on a link or download a document. Remind your staff not to respond to messages like this - and definitely don’t download anything or click on links in unsolicited email. It’s the latest form of phishing aimed at stealing confidential data or installing malware on your network.

GOVERNMENT CHECK SCAMS
You’ve seen news stories about whether financial help for businesses might be available in the future. But remember that criminals read those headlines, too, and use them to make their phony pitches sound more credible. If someone calls or emails you out of the blue claiming there’s money available from a government agency if you just make an up-front payment or provide some personal information, it’s a phony. Our Checks from the government blog post offers tips on spotting those scams.

BUSINESS EMAIL SCAMS
We’ve warned companies about scams perpetrated via business email. For example, in a CEO scam, an employee gets a message that appears to come from a company higher up directing the person to wire money, transfer funds, send gift card codes, etc. In reality, a real email

Blog Posts
- New funding for Coronavirus SBA loans attracts scammers
- What’s at the intersection of COVID-19, cancer claims, and CBD? This FTC case
- New FTC warning letters cite unsupported Coronavirus-related health and earnings claims
- 21 more companies warned about questionable COVID claims
- First FTC coronavirus lawsuit alleges company lured consumers with false SBA connection
- Small business financing: Considerations for borrowers and lenders during the coronavirus crisis
- Thinking about making Coronavirus claims? Read the latest FTC warning letters first.
- COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus
- Joint letters take new steps to stop illegal Coronavirus robocalls
- Small businesses: Where to go for financial relief information
- Seven Coronavirus scams targeting your business
- Where small businesses can turn for accurate information about financial relief
- New Coronavirus warning letters: Who can it be now?
- FTC, FDA warn companies making Coronavirus claims
FTC v. Ponte Investments, LLC (complaint filed)
FTC v. Whole Leaf Organics (complaint filed)
Subscribe to the FTC Business Blog Alerts for the latest on COVID-19 and data security law enforcement, ftc.gov/subscribe

Visit ftc.gov/coronavirus for the developments

Share FTC resources on your site and in social media

Contact me at lfair@ftc.gov
Jon Clay
Cybersecurity Expert and Director of Global Threat Communications
Trend Micro

William Malik
Vice President, Infrastructure Strategies
Trend Micro

https://resources.trendmicro.com/Coronavirusresources.html#News
Threats Using Coronavirus as Lure
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
- 220x Increase in spam from Feb to Mar 2020
- 260% Increase in malicious URL hits from Feb to Mar 2020

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

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period January 1 to March 31, 2020).
Map of threats using COVID-19 – Q1’2020

This data reflects findings until March 27, 2020
**Emotet** was discovered in 2014 from a known banking malware variant that stole data by sniffing out network activity. It evolved into a more complex form, acting as a loader for other malware families.

**EMOTET** was prominently used in coronavirus campaigns.

---

**EMOTET Infection Diagram for the recent wave of attacks**
SPAM: top method to deliver attacks on enterprises

94.9%

Top 2 Spam Samples

- Shipment Notification
- Coronavirus Ministry of Health Updates
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 are I capable of doing?
If I want, I could infect you and your whole family with the Corona Virus (COVID-19).
Delete all your secrets. There are countless things I can do.

What should you do?
Transfer the amount of $500 in my bitcoin address (if you do not know how to do this, write to Google: “Buy Bitcoin” or https://www.cryptocurrency.org).

My bitcoin address (BTC Wallet): 1HEGd9pZwZXcNgPQocykvBZJnjA6iAlI

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

I give you 72 hours (NOT more than 7 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 replicaing the email because it was sent from your system and email account.

If I think that you have shared this message with someone else or try to spread this, then YOU and many members of your family will be infected with the Corona Virus (COVID-19).

Coronavirus extortion email spam

---

**Expected growth in EMAIL SCAM proliferation**

**Top Emerging Techniques**

1. Targeting specific countries, including China and Italy
2. Business Email Compromise
3. Cruel ransomware
4. Sextortion-related scams
Threat actors exploit the public’s need for information about Covid-19 to distribute malware.

INFO-THEFT THROUGH CORONAVIRUS INTERACTIVE MAP

An interactive coronavirus map was used to spread information-stealing malware.

MALICIOUS MOBILE APPLICATION

A mobile ransomware named CovidLock comes from a malicious Android app that supposedly helps track cases of COVID-19.
Threat actors exploit the public’s need for information about Covid-19 to distribute malware.

**FAKE COVID-19 SAFETY PORTAL FROM THE WORLD HEALTH ORGANIZATION (WHO)**
Phishing site that pretends to be a WHO portal.

**FAKE CENTER FOR DISEASE AND PREVENTION WAITLIST**
Another phishing site aiming to get personal information.
Social Media Scams

We offer you Netflix for free. Staying safe and enjoying the Internet at home. See what’s next.

Total cases: 1.6m
The coronavirus’ effects have reached the CYBERCRIMINAL UNDERGROUND.

Popular Items Now Sold in the Underground

- Covid-themed phishing, malware, and exploits
- Toilet paper, N95 masks, ventilators, and other essential supplies
Best Practices
Layered Messaging Security

Multi-layer Threat Prevention

Internet

Email Sender Reputation
Pre-execution Machine Learning
Anti-Malware – Static
0-Day Malware – Behavioral
Macro Detection
Document Exploits
Social Engineering Protection
Writing Style DNA
Credential Phishing Attack Protection
Gateway Web Reputation
Filter by File Type or Extension
Click-time Web Reputation

Sandbox Analysis
Best Practices – User Security

- **Passwords**
- **Email Safety**
- **Online Safety**
- **Remote and office**

- Cyber defense is no longer just behind your home or business network firewall
  - ✓ Protecting your *data* is a must (versus just perimeter)

- Be cautious with public Wi-Fi
  - ✓ Disable auto-join or auto-connect to popular public WiFi AP (i.e., airports, coffee ships, malls, restaurants)
  - ✓ Understand how to use VPN and https

- Cloud service security and backup setup
  - ✓ (One-Drive, Google Drive, Dropbox..etc.)

- Back-up strategy and process *<= Important*
  - • On-premise and/or cloud
How long would it take for an attacker's computer to crack the following passwords?

"clubpipe"
"clubp1pe"
"clubpipewave"
"Clubp1pewave"
"clubpipewavebarking"
"Cloudp1pewaveb@rknig"

Source: Trend Micro
How long would it take for an attacker's computer to crack the following passwords?

"clubpipe" = 5 seconds
"clubp1pe" = 1 minute
"clubpipewave" = 4 weeks
"Clubp1pewave" = 3 thousand years
"clubpipewavebarking" = 16 billion years
"Cloudp1pewaveb@rknig" = 43 quintillion years

Source: Trend Micro
Best Practices – Device Security

- **Computers/Servers**
- Mobile Devices
- Wi-Fi Routers
- Other Devices

- Centrally managed, business grade cybersecurity software coverage for cloud, web, email, server and network security
- Ability to mitigate and recovery from a breach or cyber attack such as Ransomware
- Isolate payment systems (home vs. work PC)
- Restrict access to servers
- Implement two-factor authentication
- Update software/firmware regularly
Best Practices – Device Security

- Computers/Servers
- **Mobile Devices**
- Wi-Fi Routers
- Other Devices

- Update operating system and apps regularly
- Use built-in security features
- Turn off any app permissions you do not use
- Minimize location access
- Disable Bluetooth when not required
- Do not connect to unsecured Wi-Fi networks
- Only download apps from trusted sources
- Ignore and block unsolicited calls and messages. Do not return calls from unknown numbers
- Use long, strong passwords
- Minimize personal data in apps and websites
- Consider using a vendor security product
Trend Micro deployment shifts over time—from on-premises to SaaS-based solutions. Created with real data by artist Stefanie Posavec.
Patrice Bobola
Head of Global IDP Knowledge & QA
Generali Global Assistance

www.irisidentityprotection.com
Top Tips to Minimize the Risks

1. Check who the sender is
2. Take a careful look at any email that requires an action
3. Do not click the links or open attachments from unfamiliar senders
4. Check the email for grammar and spelling mistakes
5. Confirm all requests for sensitive information via phone or in-person
6. Be careful with the information you disclose
7. Avoid opening emails you did not request
8. Invest in a strong spam filter solution
9. Provide ongoing employee training for phishing, social engineering, & other common types of scams
Precautions to Take to Avoid Cyber Threats

1. Create strong & unique passwords
2. Consider using a multi-factor authentication tool
3. Invest in a strong spam filter solution
4. Before changing a password, verify your account recovery settings
5. Use non-honest answers for online account security questions
6. Visit the website directly to verify any account notification and/or alert
7. Consider your payment type when making online purchases
8. Do not store your bank information on less familiar websites
9. Talk to your peers & community about potential scams
10. Provide ongoing employee training
11. Report scams to the FTC at www.FTC.gov/Complaint
Additional Resources

NCSA’s COVID-19 Library

Avoiding Cyber Threats and Scams
- CISA: Defending Against COVID-19 Cyber Scams
- CISA: CISA Alerts and Recommendations
- CISA: Recommendations on VPN Security
- Cofense: Coronavirus Phishing Infocenter
- ESET: Beware Scams Exploiting Coronavirus Fears
- FTC: Tips for Avoiding Coronavirus Scams

Security Tips for Working Remotely
- CrowdStrike: Cybersecurity in the time of COVID-19: Keys to Embracing (and Securing) a Remote Workforce
- Cyber Readiness Institute: Securing A Remote Workforce
- EDUCAUSE: Resources for Business Continuity and Alternative Education Delivery
- EDUCAUSE: Corporate Resources for COVID-19
- ESET: COVID-19 and the Forced Workplace Exodus

Government Assistance and Other Guidance
- CDC: What You Need to Know About COVID-19
- EDUCAUSE: Student Privacy during the COVID-19 Pandemic Whitepaper (PDF)
- IRS: Coronavirus Tax Relief
- SBA: SBA Disaster Assistance in Response to Coronavirus
- WHO: Coronavirus Disease (COVID-19) Outbreak
Upcoming Webinars

- **May 12**: Phishing, Vishing & Smishing
- **May 26**: COVID-19 Scams
- **June 9**: Telework Security
- **July 14**: Business Identity Theft

Register here: https://staysafeonline.org/event_category/cybersecure-my-business/
Q&A

Lesley Fair
Senior Attorney
Bureau of Consumer Protection
Federal Trade Commission

Jon Clay
Cybersecurity Expert and Director of Global Threat Communications
Trend Micro

William Malik
Vice President, Infrastructure Strategies
Trend Micro

Patrice Bobola
Head of Global IDP Knowledge & QA
Generali Global Assistance

(MODERATOR)
Daniel Eliot
Director of Education & Strategic Initiatives
National Cyber Security Alliance

*This webinar will be recorded and will be distributed to registrants after the webinar concludes*