Coronavirus Crimes

Imagine this visual: A cool, clear pool of water out on a hot, dry savanna. Graceful gazelles, first one, then two, then nearly thirty of the gorgeous creatures come and bend their necks down to drink. In the distance there comes a deep rumbling, and the gazelles raise their heads to listen. Then a loud crack of lightning strikes, to go along with the once distant rumbling, distant no more but splitting the trunk of a tall tree at the water's edge. In that moment of distraction and chaos, as the gazelles turn to run…the predators emerge from the shadows at the edge of the pool, having been waiting there all along, hidden from their prey. The hyenas give chase, and in those moments of fear and confusion, they rip the throats of their prey, laughing as hyenas do.

In this scenario, the coronavirus cons are the hyenas, laughing after the kill. You, sadly, are the gazelle.

Door-to-Door Coronavirus "Tests"

Let the camel's nose into the tent and his tail will surely follow!

Meet the new generation of door-to-door "salesmen" and -women. No, not vacuum cleaners, not encyclopedia sets, but fake coronavirus "test" kits. Do not open the door. Repeat: *Do not open the door!*

It's been reported that some of the perps present themselves as law enforcement or even the Red Cross! Police departments across the country are sounding the alarm about scammers going door-to-door, to *your door*, pretending to perform in-home tests for the coronavirus. Multiple public health departments in municipalities dotting the map have repeatedly announced

they will never, ever, go door-to-door or perform in-home COVID-19 tests, but those announcements aren't working. The scams go on, and they're working.

Fake door-to-door COVID-19 testing is dangerous on so many levels. First, there is currently no such test, so the test itself is bogus. The premise of door-to-door sales calls is an old tried and true "distraction robbery" scam. In other words, the "salesman" knocks or rings your doorbell, then distracts you by getting you to answer the door and listen to a sales pitch, thus getting a toe in your door, literally. Next, the "salesman" manages to get his or her entire body in your home, further distract you with some bogus health test, then robs you or even worse.

Another threat is that you may actually buy the fictitious test, meaning your credit card information has been stolen!

Testing for COVID-19 is an extremely serious undertaking. If such a test were genuinely performed, the medical professional conducting the test would be draped head-to-wrist-to-toe in medical garb to protect both you and them from potential contamination. Door-to-door COVID-19 testing is a no-go simply because of the highly contagious nature of the virus itself.

As of this writing, there is no such thing as legitimate door-to-door coronavirus testing. No one from the Centers for Disease Control or the municipal departments of health makes house calls to offer tests for a fee. In North Carolina, door-to-door perps were offering not only COVID-19 test kits but cleaning supplies to fight the virus as well. It's happening, and it's happening now. From North Carolina to Arkansas and Palm Beach, door-to-door "testing" has been reported.

U.S. Customs and Border Protection has released a photo showing a package of counterfeit COVID-10 "test kits" that had just arrived from the U.K. at the Los Angeles airport. The package contained six clear plastic bags, each full of vials of a white liquid labeled CORONA

VIRUS 2019NCOV (COVID-19) and VIRUS1 TEST KIT. The package was handed over to the FDA for testing.

Scammers are taking advantage of the global pandemic, smuggling counterfeit test kits, going door-to-door donning white suits and face masks, and claiming to be from a health agency. The FBI issued a warning advising consumers to beware.

At a time when many of us are quarantined, sheltering at home, or self-isolating, you'd think we were safe behind closed doors. Not exactly. Instead of being safer at home, con artists see us as being *trapped* in our own homes. For them, it's like shooting fish in a barrel—they can't miss.

For years, I investigated, prosecuted, and covered home invasions, burglaries, and assaults in the home. Here are some of my golden rules:

- Look before you open! I grew up in a rural setting, and we always flung our doors open whenever there was a knock or the doorbell rang. With neighbors few and far between, excitement pulsed through the house whenever we had a visitor. In 2020? Not true. And that is why I recommend peepholes on front doors of homes and apartments, especially the kind with a little sliding cover on the inside so there's no way anyone on the outside can look in.
- If you do not have a peephole, take a look at who's knocking from a side window or some other vantage point in your home.
- Think about it: With social distancing, curfew, lockdowns, or quarantines in place, how likely is it that someone approaching your home or apartment unexpectedly is who they say they are? That likelihood is low to zero.

- Now we have the awesome Ring Video Doorbell and its progeny. The Ring connects to your WiFi (you may need a booster), and the moment the doorbell "rings," the image of who is there pops up on your smart phone. We have them installed at both doors, and I love them. If a fake medical professional comes to our door wearing a doctor's costume, we can see him/her coming and call 911 pronto.
- Modern home security systems often come with a wireless keychain alarm. Keep one near your door or take it with you when someone knocks. Press it if you need to call for help. An ounce of prevention is worth a pound of cure.
- Home security alarm keypads are often placed in master bedrooms and near doors for a reason: so you can reach them at the most likely places for an emergency or security breach to occur. Be familiar with the pad, including the emergency button. When that knock comes at your door, know how to use it. Keep your home security alarm on even when you are home. As a matter of fact, keep it turned on *especially* when you are at home. You can get a new TV. But you can't run over to Best Buy and get a replacement for *you*.
- If you do not have a home security system, take your cell phone or cordless when you answer the door in case you need to make an emergency call.
- Fortify your doors! Deadbolts are preferred The more force a door can withstand, such as kicking or battering, the better. Don't install deadbolts that require an inside key because if you need to get out quickly, you don't want to be fumbling for that key. Seconds count.

- If for some reason and against my strong advice, you follow your impulse to answer the door, do not—repeat, DO NOT—invite or let the person into your home. If they convince you to use your credit or debit card, you have given them the keys to the kingdom, your life savings. Worse, you have set yourself up for a home robbery or an even more serious felony.

Please, don't do it. Once you turn that knob and open the door, it's too late.

Fraudsters Take to the Airwaves to Peddle Coronavirus "Snake Oil"

As of this writing, there is no cure, no antidote, and no vaccine to eradicate or stop the virus once contracted. But in a time of fear and chaos, many people will try anything to protect themselves, their children, and their family. And believe me, fraudsters are only too happy to help them out…out of their money!

Bringing coronavirus "cures" to the forefront was none other than the world famous televangelist Jim Bakker. Bakker took to the airwaves again, amidst the panic and fear of the virus.

Long before coronavirus had ever hit the headlines, Bakker ruled a multimillion-dollar business as a televangelist alongside his wife, Tammy Faye. They quickly adopted a lavish lifestyle, including minks and troves of expensive jewelry for Tammy Faye, a fleet of Cadillac limos, a vintage Rolls Royce worth over $60,000, multiple mansions, and a houseboat. I remember what particularly caught my attention at the time: an air-conditioned dog house for their animals and $9,000 worth of truffles the two had allegedly flown in from Brussels for a party.

Jim and Tammy Faye Bakker danced to the music all right, but who paid the piper? The churchgoers and followers of Bakker's ministry, that's who. After a sixteen-month grand jury investigation, Bakker was indicted in 1989 for defrauding his followers out of millions in donations and, later, convicted and sentenced to forty-five years in a federal pen and half a million dollars in fines.

Bakker somehow finagled a reduced sentence and walked out of jail in 1994. It didn't take long for people to forget Jim Bakker assuming a fetal position and sobbing on the floor of the courtroom during his trial. You'd think he would've learned his lesson, right? Wrong.

As soon as he could, he went straight back on the airwaves, and when COVID-19 hit the headlines, Bakker took to the stage as well, this time hawking a concoction called "Silver Solution" as a cure for the virus. Gazing out to his viewers, Bakker glanced back at a silver-and-blue bottle. Questioning a "natural health expert," Bakker elicited the punchline: that an eighty-dollar, four-ounce silver-and-blue bottle "totally eliminates [coronavirus], kills it, deactivates it." Bakker's guest went on to claim that Silver Solution, simple colloidal silver, "has been proven by the government that it has the ability to kill every pathogen it has ever been tested on, including SARS and HIV."

The state of Missouri has filed a lawsuit claiming Bakker, along with Morningside Church Productions, violated state law by "falsely promising that Silver Solution can cure, eliminate, kill or deactivate coronavirus and/or boost elderly consumers' immune system and help keep them healthy when there is, in fact, no vaccine, pill, potion or other product available to treat or cure coronavirus disease 2019." Following Missouri, the New York attorney general ordered Bakker to cease-and-desist making his claims and accused him of defrauding the public.

The FTC and the FDA have both warned Bakker that his Facebook page and website were selling "unapproved" new drugs in violation of the law.

The FDA also sent warnings to six other companies caught selling colloidal silver essential oils, teas, and treatments. Not only does colloidal silver not cure the deadly coronavirus, it can actually be dangerous to your health, according to the National Institutes of Health.

Jim Bakker isn't the only one making money off fear and desperation. Straight from big-screen productions like *Iron Man 2, Thor,* and *Moneyball*, Hollywood actor Keith Lawrence Middlebrook went public to announce that he had personally developed a "patent pending cure" for COVID-19. He also claimed NBA superstar Magic Johnson was on his company's board of directors. Not only was Middlebrook conning the public into sending him money for a fake cure, he was also seeking massive money investments. But I don't want to paraphrase it, I want you to hear it straight from the horse's mouth. Let me quote Middlebrook directly.

"I have developed the cure for the coronavirus COVID-19…[An] LA patient tested positive for coronavirus, got up and walked out fifty-one hours after my injection." But Middlebrook couldn't stop himself and allegedly went on: "Investors who come in at ground level, say $1M, will parachute with $200M–$300M…conservative minimum."

Don't worry: Middlebrook was arrested during a meeting when he delivered a batch of coronavirus "cure" pills to an investor who, of course, turned out to be an undercover FBI agent, according to the Feds.

The U.S. attorney for the Central District of California, Nick Hanna, gave a statement after the sting. "During these difficult days, scams like this are using blatant lies to prey upon our fears and weaknesses. While this may be the first federal criminal case in the nation stemming from the pandemic, it certainly will not be the last. I again am urging everyone to be extremely

wary of outlandish medical claims and false promises of immense profits. And to those who perpetrate these schemes, know that federal authorities are out in force to protect all Americans, and we will move aggressively against anyone seeking to cheat the public during this critical time."

Middlebrook was charged with felony attempted wire fraud. He's looking at a possible sentence of twenty years in a federal pen. And the final humiliation for the actor-turned-con? Magic Johnson says he's never heard of Middlebrook. Ouch.

Wow. If you can't believe a Hollywood star from *Iron Man* and you can't believe a preacher, who can you believe? Maybe a famous conspiracy nut? Like Alex Jones, who still insists the mass shooting at the Sandy Hook Elementary School didn't happen? But believe it or not, Jones still has a huge audience, and this is what they heard.

Jones's home platform has long been the website Infowars, various "news" blogs, video feeds, an online store, and audio, all founded by Jones. One day after the popular Austin, Texas, festival South by Southwest was called off over coronavirus fears, Jones hyped that the cancellation was really a secret government psychological operation meant to create panic. Jones then stated: "But having antivirals, getting your immune system healthy—that is the answer. And, yes, folks, we sell great antivirals."

Jones's online "health" store hawks products chock full of colloidal silver, with catchy names like SuperBlue Toothpaste, SuperSilver Wound Dressing Gel, DNA Force Plus "supplements," and SilverSol gargle. Jones claims the products can protect against or even treat the novel coronavirus. In one live production in mid-March, Jones went so far as to promise that "this stuff kills the whole SARS-corona family at point-blank range…it kills every virus."

The New York State attorney general, Letitia James, brought the hammer down on Jones, stating: "Whenever there's heightened fear and hysteria, we start to see scammers…As the coronavirus continues to pose serious risks to public health, Alex Jones has spewed outright lies and has profited off of New Yorkers' anxieties. Mr. Jones's public platform has not only given him a microphone to shout inflammatory rhetoric, but his latest mistruths are incredibly dangerous and pose a serious threat to the public health of New Yorkers and individuals across the nation." She promptly ordered a cease-and-desist letter to Jones.

And that's not all. According to *Business Insider* and citing *Wired*, Google removed the Infowars Android app from its Play Store immediately after video surfaced of Jones arguing against sheltering in place, quarantines, and social distancing in the war against coronavirus. The timing was quite the coincidence.

I say good riddance to Jones. You go ahead and gargle with SuperBlue, Jones. I plan to stick with the World Health Organization.

Coronavirus "Purell Pirates" Go Price-Gouging, Aaargh!

By now, millions of us have heard the true story of the so-called "hoarding bros," a pair of Tennessee brothers who, before now, had an unblemished record and a great reputation. That said, brace yourselves.

Just twenty-four hours after the announcement that the coronavirus had claimed its first American victim, two Tennessee brothers, Noah and Matt Colvin, took to the road. Their road trip first took them to one of my favorites, the Dollar Tree. With bags loaded, they then wheeled over to Walmart, Home Depot, and more. At each pit stop they bought every bottle of hand-sanitizer in sight.

After three days, having wound their way through Tennessee and Kentucky, they'd packed a U-Haul truck with *thousands* of hand-sanitizer bottles and *thousands* of antibacterial wipes, cleaning out supplies for miles and miles. It's believed the two had amassed nearly eighteen thousand bottles of hand-san! The "hoarding bros" then posted hundreds of bottles of hand-sanitizer online *for up to $70 each!* Good business? Or plundering…making money off despair?

In another case, a forty-three-year-old Brooklyn man, Baruch Feldheim, is now facing assault charges on FBI agents. Eek. Over hand-sanitizer? How did it all start? It started when Feldheim allegedly sold a Jersey doctor, desperate for medical supplies, a thousand N95 face masks for a whopping $12,000! That's nearly a 700 percent markup!

But that's not all! Feds say Feldheim then sent another doctor to a New Jersey auto repair shop to hook him up with a load of medical and cleaning supplies. You know there's a problem when you're selling supplies out behind the local car repair shop. The doc reportedly told the Feds that Feldheim hoarded enough Clorox wipes, hand-san, face masks, chemical cleaners, and surgical supplies to outfit an entire hospital. Think *eighty thousand* face masks, according to reports.

To make matters worse, when the Feds showed up to effect a search warrant for hoarding medical supplies and price gouging, court docs say Feldheim blurted out he was infected with COVID-19 and proceeded to intentionally cough on the agents. Feldheim should've heeded the sage advice from Jim Croce: You don't tug on Superman's cape, and you don't mess around with Jim—or FBI agents searching your garage.

Crossing the country to Phoenix, the local CBS station reports that not only doctors but firefighters and police are getting ripped off by coronavirus pirates! Two congressmen, Ruben

Gallego and Greg Stanton, went to the FTC and the U.S. attorney general calling out, as they described it, shameful and un-American conduct. If they are right, then I, for once, agree with the politicians! They claim a local company has drastically jacked up prices, charging the Phoenix police and fire departments a *500 percent markup* for N95 face masks! And police and firefighters are being gouged!

Oregon has also suffered. In March, when coronavirus fears first struck many of us, store shelves were being picked clean. According to the *Salem Statesman Journal*, a Keizer Food Mart removed single rolls of toilet paper from commercial packages of multiple rolls, *selling a single roll of TP for $3.99.*

The store manager insisted his employees were trying to "help" customers. After much public shaming, a price-gouging cease-and-desist letter was issued by Oregon's department of justice. The store was one of seven Oregon businesses and 7-Elevens that allegedly jacked up prices on toilet paper, surgical face masks, and even bottled water.

Price gouging has been reported on eBay as well, with complaints that disinfectant sprays like Lysol were selling for hundreds of dollars each! The California attorney general blasted the greedy sellers as not only disgraceful but illegal…and he's right!

But how can we fight back?

- Plan ahead. Know what you need before you go empty, so when you see it, make the purchase. Do not hoard…just purchase. I know how it feels: When I saw Clorox wipes being unloaded off a truck in the grocery store parking lot, I considered a car-jacking. I didn't, and I bought only two packages.
- Rely on trusted sellers. Beware, because while shopping online may save you from the crazy crowds, at your local grocery store, Target, or Home Dept, you

at least know who you're dealing with. I haven't seen a single report that, for instance, Target or Walmart has been accused of price gouging.

- Check customer reviews on the seller before you submit your credit card or PayPal info. Once you click, it's too late!
- Be extra careful if you end up dealing with third-party vendors you don't know or have never heard of.
- Carefully read labels. For instance, in the mad rush for hand-sanitizer, lots of people ended up with gel containing a reduced amount of alcohol. To be effective, hand-san has to contain at least 60 percent alcohol to work against COVID-19, according to the CDC. I know lots of labels say the product "kills 99.99 percent of illness-causing germs," but that does NOT guard you against coronavirus.

Washing slowly with soap and water (then NOT touching your face or biting your nails) is the single most effective way to get rid of tactile coronavirus germs, but that's a different can of worms.

As to labels, know that "alcohol-free" products or those containing less than 60 percent alcohol are not recommended by the CDC. Many hand-sanitizers (Germ-X and Purell) use benzalkonium chloride instead of alcohol. They may not work as well against the coronavirus, says the CDC, although they are better than nothing. Bottom line, read the label before you buy. Study the product image. If an online vendor doesn't display a product image, don't buy it.

P.S. Don’t make homemade hand-san out of vodka! Whiskey and vodka don’t have enough alcohol content to work, no matter how much it burns going down your throat. And don’t even mention moonshine.

- If you are shopping online and the price doesn’t make sense, you may consider price-checking tools. They are free to you and track the product’s price history. Two examples are Camelcamelcamel and Keepa. They can also alert you if there is a price drop. Nice.
- If you think you are being price-gouged, take a photo of the price and your receipt, signs, or price tags. Hold on to them.

It helps if you have photos or proof of comparative prices as well, such as what another store or vendor is traditionally charging for the same product. Get the name and address of the suspected price-gouger. Then call and send copies of your evidence to not only local police, but your state’s attorney general, the state’s consumer affairs division, and the Better Business Bureau. Keep a written list of the dates and times of your calls and with whom you spoke.

Fight back against the price-gouger pirates! We don’t allow bloodthirsty pirates on the high seas and we shouldn’t tolerate them online or at the grocery store either!

Coronavirus Robocalls

What if you, you mother, dad, grandfather, or grandmother got the following call?

“The coronavirus has caused the U.S. to declare a national emergency. The Families First Coronavirus Response Act has made coronavirus testing more

accessible immediately. If you want to receive a free testing kit delivered overnight to your home, press one."

"This is a courtesy call from 3M's safety program to inform you that due to the coronavirus pandemic, the government has authorized our laboratories to offer you the safety and medical kit, which at this moment is sold out in the market. We are giving you the priority to have access to the supplies needed before the states lock down."

"Greetings. This is an automated message alert from the Worldwide Health Organization to inform you about the EPA's Emerging Viral Pathogen Program for the coronavirus protection. We offer you the opportunity to obtain the most powerful and secure protection equipment to protect yourself and all of your family members."

"Thank you for calling the coronavirus hotline. Because of the limited testing we are first taking Medicare members. Will the free at-home test be just for you or for you and your spouse?"

The above are actual examples of "robocalls"—some even repeated in fluent Chinese—made to unsuspecting consumers on their private numbers, people who, like the rest of us, are watching hospital beds fill up as the world coronavirus death toll rises each day. People just like you and me, who will do anything to keep our families safe.

Robocalls are, very simply, unsolicited calls from scammers to trick you into handing over your credit card information in exchange for either a bogus product or absolutely no product at all. And I'm not talking about some lonely guy in his basement making random calls—this is big business, and their attack plans are calculated and cold, raking in millions. Once you give

them your banking info, the con on the other end of the line proceeds to raid your accounts, wreck your credit, and more. You can actually hear the calls above and many more just like them at NoMoRobo, a robocall blocking website.

Fear and panic, fueled by 24/7 news hysteria, has spawned countless robocall scams. From lotteries to get a COVID-19 cure to air-duct sanitizing to fake insurance and virus "cures," the calls are relentless. Some estimates are that, since the pandemic started, one million coronavirus calls are made every single day, scaring those who get the call and taking advantage of their fears and lack of real information.

How can you fight back against low-life coronavirus robocalls? Here's how:

- Hang up! The moment you realize you don't recognize the voice on the phone and that voice mentions the coronavirus in any form—be it insurance, a loan, a vaccine, or a face mask—don't wait to say goodbye. Don't worry about being rude, just hang up. Would you worry about being rude to an armed robber? They may not have a gun, but the caller is using coronavirus as a weapon…against you! Hang up!
- Don't wait to speak to someone to tell them how much you hate unsolicited calls or find out if the product is legit. It's not.
- For Pete's sake, don't buy anything or give out any of your information!
- Don't press any numbers, make any "menu" selection, or even press a number to "end the call" or "remove you from the call list." While the recording might tell you that pressing a number will direct you to a live operator or some other choice, pressing a digit may very well lead to even more robocalls to your

number. Consider apps like RoboKiller, Hiya, YouMail, Mr. Number. and NoMoRobo.

- Don’t fall for calls boasting a coronavirus vaccination or testing kit. As of this writing, there is no coronavirus vaccine, treatment, or authorized home-testing kit. Go to the FDA website to read more.
- If you truly believe a phone solicitation, fact-check the information before you hand over your credit card.
- Never respond to any call about getting money or checks from the government. Federal government coronavirus benefits are not yet finalized.
- Don’t take calls from the CDC. Why? Because the Centers for Disease Control and Prevention or any so-called “experts” aren’t cold-calling you. They are in their research labs trying to find a cure or vaccine. For the very latest coronavirus info, go to the CDC or WHO website.
- Don’t fork out for charities, donations, or crowdfunding that cold-call you. It’s highly likely they are not who they say they are. If you want to contribute, God bless you. Go to a legitimate charity like UMCOR, UNICEF, or the Red Cross. Make that donation count—don’t line the pockets of a con artist or robocall behemoth sites.
- Don’t fall for robocalls pitching loans or even health insurance for coronavirus treatment expenses or services that claim to sanitize your home and “clean” away COVID-19.
- Know that robocallers can “spoof” or jigger with the caller ID number that pops up on your phone’s screen, making it appear to be a number you may know,

such as from your area code or using the first three digits of your neighborhood phones. That's called "neighbor spoofing," and it makes you think you recognize the number.

There is a way to authenticate caller ID. The application is called Stir/Shaken, and it can block certain calls such as masked numbers that trick you into answering and eliminate spoofs. One drawback is that it doesn't work with international calls.

- Your phone itself can actually fight coronavirus robocalls, as many handsets now have built-in robocall blockers. Investigate whether your phone does. Go to Google and find the customer service number for your model phone. Call it and ask!
- Google has a new tool named Call Screen that comes in many of its smart phones. When you get an incoming call, tap "screen call." Google Assistant answers for you and asks the caller to ID themselves and give the purpose of their call. Then a transcript of the response pops up on your phone for you to see it. If it's a robocall, you can block the number from calling you again.

Rule of thumb? Ignore incoming calls from any number you don't recognize. And never press a number even if some automated voice tells you to!

Phishing, Email and Text Scams, and Fake Online Ads

Phishing…what is it? Well, it's not with a line and pole, I can tell you that! In the criminal "phish-tank," the con man has the hook and you, sadly, are the little guppy swimming in a pool of coronavirus fear.

Simply put, phishing is when a perp uses a phony name or entity and sends you emails, texts, or ads that entice you to pass on critical personal information such as your credit card number complete with security code and expiration date, debit card info, or banking details such as an account number. Victims are also tricked into providing log-in numbers, home or business addresses, and even social security numbers.

Yes, I know it sounds outrageous and you think that could never happen to you, but it does. These emails look so perfectly legitimate that even an eagle-eyed consumer could fall for them! And if you do, the perps end up with your information, your location, your money, credit, and maybe even your identity. Phishing emails can even worm in and gain access to your computer and accounts, such as your email account. They can install ransomware that lock you out of all your data or malware that infects your computer and accounts with destructive bugs.

In the time of coronavirus, it works like this: Cybercriminals email, claiming to be a legitimate entity passing on COVID-19 information. The email may direct you to open an attachment such as a list of safety measures, a coronavirus map, emergency procedures, shortage alerts, or statistics. The attachment could purport to be any number of things.

Once you click on the link or attachment, you unwittingly download malicious software, known as “malware.” That malware gives the cybercriminal control over your computer to access all your information and even log each and every one of your keystrokes. The download contains a virus that can then monitor all activity on your device, be it tablet, phone, laptop, or hard frame. If you log in to work, the perp or malware runs through the company’s system as well.

How do they do it? How do they outsmart you? By posing as familiar company names or pretending to be someone you may know. It happened to me when I got an email from someone

who purported to be American Express. The email looked almost identical to a real American Express email. It had the same pale blue colors and logo. It looked the same! But it wasn't!

My brother even got a fake court summons about a nonexistent case! That's bold! Now, amidst fear, anxiety, and uncertainty, cybercriminals are using coronavirus to their own advantage. Some are even stooping to send missives from the CDC or WHO, the World Health Organization.

Not surprisingly, coronavirus phishing is morphing by the hour, already assuming mew forms. Some phishing scams even include warnings, like "You are immediately advised to go through the cases above for safety hazard." According to Consumer Reports, fake emails apparently from the WHO or CDC offer new updates about COVID-19, suggest an available vaccine or treatment, even claim to be a coronavirus victims charity. That's low.

Oftentimes, recipients are so concerned about the virus that they don't notice details that may otherwise ring a bell of alarm, like poor grammar or spelling mistakes. Also, right now there is a flood of legitimate coronavirus news and information being disseminated by the media, employers, schools, and vendors. The cyber perps hope to get lost in the jungle of legitimate data and ambush you to get a click.

A new ruse, phishing emails seemingly from your company HR, are on the rise. They want you to log on, and once the perp gets your log-in or password, it's over.

And now, headed our way is a brand new scam originating out of the U.K. Thousands of Brits got scary coronavirus texts from the "Government" informing them they'd been "fined" for going out too much and/or straying too far from home during lockdown. The goal is to trick people who, like many of us, are under government-ordered coronavirus lockdown and acquire their credit card, debit card, or banking information. The texts, of course, are loaded with

phishing links. And people fall for them! Why? Because many of us are used to getting caught, say, by a red-light camera or the cameras on the sides of school buses that catch you sneaking around while the "stop" sign is blinking red on the side of the yellow vehicle. So when someone gets a fine for breaking curfew or lockdown, it seems real! IT'S NOT.

Fake Phishing Ads

Scammers post ads about treatments or cures for coronavirus. The ads are usually scary and urgent, playing on fears for our families and ourselves. There are only two logical outcomes of this scenario. One, click on a fake ad and catch a malware download onto your device. Two, you buy the product and receive something useless or nothing at all. Regardless of the outcome, you very well may have shared personal information with an unknown entity that you can never get back.

Bottom line? It's smart to avoid any and all ads regarding coronavirus products from toothpaste to gargles, supplements to essential oils, coronavirus cures to respirators, investments in fake coronavirus-fighting ventures to donations to fake charities. Just say no by hitting the delete button.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned us about emails with malicious attachments or links to fraudulent websites. Victims often report the subject line relates to the coronavirus. Here are a few examples.

One scam sends emails offering a coronavirus document from the "Mongolian Health Ministry." Once you click on it, malware creeps into your device. "Official" documents—often purporting to come from China, Japan, or Korea—work as a hook to get your click, and they are especially alluring during the COVID-19 crisis.

Here's another: "New COVID-19 prevention and treatment information! Attachment contains instructions from the U.S. Department of Health on how to get the vaccine for FREE." Believe me, it's not free. Click on this and it could cost you your whole bank account.

Here's another: "URGENT: COVID-19 ventilators and patient test delivery blocked. Please accept order here to continue with shipment." Don't accept it. It's not real.

There are literally hundreds more examples, but most important, how can you fight back? Here are some ways to recognize and avoid coronavirus phishing.

- BOLO! Be on the lookout for any request for your personal information. An unsolicited coronavirus email asking for personal info like an SSN or credit card numbers is no doubt a phishing scam. No legitimate health organization or government entity wants that information from you. Legitimate government agencies won't ask for that information. Don't click and don't respond.
- Look at the link and address. Hold the mouse or button over the URL. What does it say? If in doubt, don't click and immediately delete the email.
- Look for poor grammar, punctuation errors, and misspellings. It's a phish! Delete it!

I love this one: "Recommend sanitizing your docs and air filters to protect your loved ones from the Corona virus. For only $159 our highly trained technicians will do a full air duck cleaning and sanitation to make sure the air you brief is free of bacteria. So don't hesitate. Have your duck system cleaned and sanitize now."

Please, don't pay a "technician" to have your "ducks" cleaned!

- Beware of generic greetings like "to whom it may concern" or "Dear sir or madam." That's a red flag, and the missive is not legit.

- Urgent directives like “Hurry!” or “Must act now!” say only one thing: “DELETE ME!”
- Coronavirus vaccines, cures, and home test kits are not real. DELETE. Go to What the U.S. Government is Doing.com to get links to local, state, and federal government agencies to find the latest and most accurate coronavirus information.
- Don’t click on news about coronavirus-related government checks. Those details are not resolved.
- If you spot a misspelling in the URL itself, such as “COVVID-19,” it’s phishing.
- Even if the website’s URL starts with “https,” that doesn’t mean it’s safe. Look closer.
- Do not open attachments from any unknown sender.
- Turn on all your auto updates, including those on your smart phone, desktop, laptop, and tablet. Make sure they’re set to update automatically. The newest software is a must.
- Install an antivirus. I like Norton.
- If any coronavirus-related claim sounds too good to be true, it probably is.

Fake Medical Supplies, Respirators, and Face Masks Flooding the Market

Fake Supplies and Undelivered Goods

In a mad rush to combat coronavirus, part of the “armor” has become face masks and N95 respirators. They first popped up—outside the operating room, that is—in airports and on

airplanes, a leftover from the SARS scare. Now they are commonplace at the grocery store, laundry, pharmacy, and even out in the open on public streets. Counterfeit goods have been around for a long time, from money to precious jewels to name-brand shoes, clothes, purses, and perfumes—anything can be faked. But who would ever have considered *counterfeit face masks?*

It's hard to believe, but fake masks aren't just sold on the street corners or by fraudsters online. In a very disturbing twist, Holy Name Medical Center in New Jersey was sent a total of one thousand N95 masks from a known vendor they'd worked with for some time. Holy Name is at the forefront fighting the coronavirus, so it was a shock when the hospital discovered the masks were fakes. According to NJ.com, the hospital's PR director, Jessica Griffin, stated the hospital has a policy of testing medical equipment before using it. She said the masks "did not fit the face area properly" and were not marked with specific Centers for Disease Control and Prevention approval labels.

There are three main categories of face mask: an ordinary face mask, a surgical face mask, and a respirator mask.

Ordinary masks are the thinnest. They are meant for day-to-day activities like cleaning and in no way do they provide proper filtration of particles and micro organisms. Although by far the most comfortable, ordinary masks are the least effective in protecting you from a contagious virus. A surgical face mask, also loose fitting, covers the mouth and nose. It typically is 3-ply and has two loops to stretch behind the ears, holding the mask over the face. Face masks catch larger particles and/or droplets. A respirator is tighter fitting and creates a facial seal to filter anything inhaled or exhaled by the wearer. A respirator provides the wearer more protection than does a face-mask. There are three types of respirator masks: the disposable N95, the half face, and the full face.

In the time of coronavirus, face masks and respirator masks are in such demand that a huge black market in counterfeit masks has developed. Fakes do not provide the same level of protection as do the real thing. Far from keeping you safe, they can actually harm you, as many counterfeit face masks are made in highly unsterile conditions with zero quality control. Then you, the innocent consumer, put the fake directly over the noses and mouths of your children and family. Think about it: face masks made in the same sweat shops and basements alongside fake purses and sneakers. Except you don't inhale and exhale directly through your knockoff designer purse or the soles of your fake name-brand sneakers.

If you strap on a fake and unsterile face mask, you might as well go lick the subway straps.

But how do you spot a fake?

- Legitimate face masks are 3-ply: a translucent layer, a second white layer, and a third colored or white layer. Cut open your mask. You should very clearly see three layers. If you don't, it's a fake.
- Examine the outer box. Look for a registration certificate number. If none appears, your product is likely a knockoff.
- On the real thing, typically there will be a visible product description including the words "medical surgical mask" or "medical protective mask." If it does not have the words "surgical" or "protective," you most likely have a fake.
- If you have 3M masks, simply check the anticounterfeit code on 3M's public WeChat account.

- Real respirators are form-fitting, made from fibrous material, and, like the N95 name suggests, filter out 95 percent of airborne particles. Fakes are pieced together with cloth and look more like surgical masks.
- Surgical masks protect from coughs and sneezes. Logically, the outer layer is waterproof! Test it: Fold your mask like a taco, then pour water into it. The mask should withstand the water, and the underside of the taco should not be damp. And the middle layer of a surgical mask is actually a filter, not just a layer of paper. If lit with a flame, it should not catch on fire as paper does.

FAKE HAND-SANITIZER

Like other coronavirus-fighting products, hand-sanitizer is in high demand. With stores and online vendors selling out of hand-sanitizer, counterfeiters are making the most of public coronavirus fears. What can you do to fight back?

- Use logic. For instance, just as you would not expect to purchase a new widescreen plasma TV at a street corner or roadside stand, neither would you expect to find legitimate, approved hand-sanitizer at such a spot.
- Be wary of new vendors that have just started offering hand-sanitizer. Why are they emerging now, in the midst of a global pandemic? There is no coincidence in criminal law.
- Make sure to read the customer ratings for online vendors. They speak volumes.
- Closely read the description online or at the vendor, including the ingredients. You may end up with jellied aloe vera or glycerin!
- Closely examine the photo online and at the vendor.

In addition to fake corona-fighting toothpastes, gargles and oils, face masks and sanitizer, other fake brands are being advertised. Some of these include MedPride gloves and SAS safety masks and fake test kits. Test kits, vaccines, cures, and treatments, as of this writing, are FAKES. Beware the burgeoning business of fake coronavirus-fighting products. Use caution!

Undelivered Goods

You go online and order coronavirus-fighting products, pay the bill, and then wait. But the products never arrive. You've either collided with major backorders or you've been scammed.

Vendors are facing high demand for medical supplies, health, and cleaning products. But remember, anyone can claim to set up shop as a vendor online using practically any name, even names that sound reliable, such as Harvard Medical Supplies or Jefferson Public Health Foundation. I just made those up. So can anyone else! That includes criminal con artists.

So what can you do to insure your vendor is the real deal?

- Go online and search for the company's or person's name, email address, physical address, and phone number.
- Look for and read the company's customer reviews.
- Check for a history with the Better Business Bureau and with the consumer affairs division of your state's attorney general's office. For a list of state attorneys general, see naag.org.
- Google the company name combined with key words like *complaint*, *fraud*, or *scam*.
- Try your best to always pay by credit card so there is a record of your purchase. If you use cash, check, or money order, there may be no way to get a refund.

- Be prepared to contest the credit charge if your items do not arrive within a reasonable period of time. If you used a credit card and you never get the products you wanted, you can at least get your money back.

Fake Charities

In a crisis like the coronavirus pandemic, cons crawl out of the woodwork. They even use your good heart and generosity to steal. Beware of charities springing up around the coronavirus. Fake charities may purport to be raising money for victims or research or somehow fighting the virus. Be careful. Not only will you lose your heard-earned savings, there's less money to give to real people in need. How to fight back?

- Some fraudsters create names that sound like a legitimate charity. Read the fine print.
- Research before you write that check. Find out who they are and what they really do to battle the virus and help those affected by it.
- Don't be hurried into a donation. If a charity insists on a cash gift, a money wire, or gift card, hold off!
- Go to nasconet.org to locate the charity regulator for your state.
- Look for information on the charity in question at BBB Wise Giving Alliance, Charity Navigator, CharityWatch, or Guidestar websites.

Lootings

Police across the country are struggling to keep the peace during extraordinarily difficult times as looters take to the streets. With shelter in place, curfews, and lockdown orders in effect,

bad guys who usually burgle private homes while residents are at work are now looking elsewhere. Easy targets? The pizza parlor, nail salon, or hardware store. All they need is a brick to break a window and they're in.

Looting is usually a mob activity and often a grab-and-go. Looters seem to believe they are entitled to steal.

Even though South Carolina governor Henry McMaster declared a coronavirus state of emergency, two men apparently thought it would be a great idea to go looting. The *Rock Hill Herald News* says the two were arrested just outside a storage warehouse unit in Lake Wylie with stolen items and a stolen truck as well. Resulting charges included burglary, larceny, conspiracy, and possession of burglary tools. Looting is now a felony since Governor McMaster declared the state of emergency.

Police in Santa Cruz, California, busted five men who allegedly set out to rob and loot businesses even though there is a COVID-19 stay at home order by the governor in effect. To add insult to injury, the looters were reportedly wearing hard-to-find surgical face masks at the time of the crimes. Santa Cruz police, already stretched to the limit, are creating a Burglary Suppression Unit to fight looting.

Boarded-up storefronts are increasing. Retailers, bars, salons, restaurants, and other establishments, with no reopening date in sight, are trying to protect themselves from looters. The *Wall Street Journal* reports that business-burglaries have risen sharply during the coronavirus emergency. There has been a 75 percent increase in commercial burglaries.

How to fight back?

- Move the most expensive material off-site for now.

- Install a security system that includes a ringing alarm as well as monitoring. They are now very affordable.
- Consider pooling the cost of a security guard with other businesses or residents in the area.
- As to individuals, stay away from retail and commercial areas as much as possible, especially at night. A would-be burglary can turn deadly in an instant.

In Conclusion

For legitimate information about COVID-19, go to the Centers for Disease Control and Prevention at www.cdc.gov or the World Health Organization at https://www.who.int.

Learn the truth about how the coronavirus spreads, prevention and treatment, known cases in the U.S., symptoms, and travel restrictions.

As of this writing, there is no cure, no vaccine, and no way to gauge the impact coronavirus will have on our families, our communities, our country, and our world. But it is possible to fight back. Protect yourself and the ones you love.

Don’t be a victim.

Keep the faith,

Ngrace