
- Editors' Note……..1
- Coronavirus Cure Claim……..2
- 2020 Security Check……..4
- 7 Reasons to Hire a Good Locksmith. 5
- Hiding in Plain Sight……6



Issue 1 | Volume 6 | March 2020


ADDRESSING THE NEEDS AND SECURING THE FUTURE

# Security Solutions

Helping secure your world

## Editor's Note

The year 2020 started most unusually, with a global epidemic – Novel Corona Virus 2019 or as we know it CoVid-2019. No one was prepared for this crisis which was first isolated in Wuhan China and which now has spread to over 120 countries globally (as of March 11th, 2020). This disease created new concerns that have created new approaches in security and how we as individuals deal with it. With the upward trend in awareness of our health, many scammers have launched campaigns to swindle unsuspecting individuals. The first article speaks about not having to buy and wear a mask or invest in companies that will supposedly make a lot of money from this crisis. And it asks readers to beware of donating to fake charities claiming to be supporting research and treatment.

The second article asks relevant questions and makes the statement; that you should make 2020 the year that you invest time and money in securing your home. It discusses home security, locks, and smart assistants. In keeping with the theme of home safety, the third articles examine 7 reasons to hire a good locksmith which range from their training, availability, insurance, and reputation.

Article four discusses stenography; this is a term that readers may not be familiar with. It's a seemingly innocent payload that controls malware that's already been installed on your computer. This is a trick that involves hiding one file inside another. More broadly, it refers to any type of information that's hidden inside something that's genuine and innocent looking.

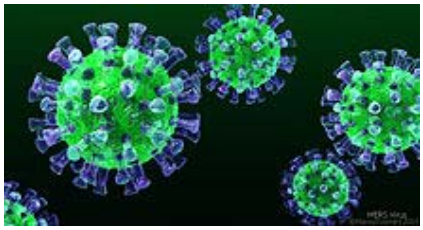
This is a threat that can have devastating effects on all files within the said computer.

We do hope you find these articles and the safety methods helpful in some manner. We at **Amalgamated Security Services Limited** will hold steadfast and continue to fulfill our commitment, which is to provide quality service for all customers.

Regards
ASSL Marketing Team

# Coronavirus Cure Claims

If you recently read about a coronavirus cure, we hope you didn't act on it. Because there isn't one -- so far at least. Nor do you necessarily need to buy and wear a mask or invest in companies that will supposedly make a lot of money from this crisis. And beware of donating to fake charities claiming to be supporting research and treatment.



We'll tell you more about these con tricks relating to pandemic disease outbreaks in this week's issue.

Let's get started...

**Coronavirus Cure Claims are Just Scams**

We'd all be delighted, wouldn't we, if someone announced a coronavirus cure? Of if there was a simple way to protect against coronavirus. Like coronavirus masks, vaccines, or pills that were guaranteed to work.

Well, as with all pandemics and global virus outbreaks, there's no shortage of people claiming they've got just these solutions. They've got the cure; they've got the drugs; they've got the protective masks. Of course, most of them are scams. As of this writing, there is no cure, not even a tested vaccine. There are no miracle pills.

And most masks offer only limited protection. For instance, if you touch an infected object and later touch your unguarded face when you take the mask off, you could still be at risk.

Wash your hands! Eighty percent (80%) of all infections are spread by touch.

We're not scaremongering, but we're highlighting the dangers of being tricked by a coronavirus scam into thinking you're safe. Ads and fake news reports making dishonest claims are spreading like wildfire.

**Social Media Carriers**

Social media networks are alarmed at becoming carriers -- not of the illness but of phony claims. In fact, Facebook has already announced a ban on ads offering a cure or preventative treatment and it looks like Google is filtering out coronavirus cure claims in online searches.

Instead, in both cases, if you search on the word "coronavirus" you'll get useful information about the illness, not dubious claims. Facebook also includes a link to the latest information from the US Centers for Disease Control and Prevention (CDC).

Amazon says it has blocked or removed more than a million products it thinks are making false claims about protection. The retailing giant has also identified and removed sellers who are price-gouging for face masks.

However, the picture is made murkier by official claims (the latest was from Vietnam) to have cured the illness, when what has really happened is that victims have been effectively nursed through the illness and emerged healthy out the other side.

In fact, that's what really does happen for most victims worldwide. We tend to read only about the deaths. There are certainly hundreds or thousands of scientists searching for a cure, but that could be a long way off. After all, we don't even have a cure for flu yet! It still kills thousands every year.

**Five Steps to Avoid a Scam**

So, while we wait for an effective vaccine to emerge, here are five key things you should do to avoid getting sucked into a coronavirus or other pandemic scam:

**1. Don't respond to any claims about cures, safety, vaccines, or other protection without first checking** with official

sources, notably the CDC. See https://www.cdc.gov/coronavirus/2019-ncov/summary.html -- this site is updated virtually every day and is the go-to source of reliable information.

But watch out for messages claiming to be from the CDC. Scammers are pitching them too. Just use the link above to get the real facts.

**2. Watch out for other email, text, and online links about news or products relating to the disease**, especially those pointing to supposed breakthroughs. Never click these links as they may lead to downloads of another virus you don't want -- computer malware.

**3. Be wary about donating to charities soliciting funds to help with research or treatment.** Always check them out first with sites like the Wise Giving Alliance (give.org), Charity Navigator (charitynavigator.org), or Charity Watch (charitywatch.org).

This may also be an opportunity for scammers to use the well-known "relative-in-distress" or "friend-in-distress" calls, which trick victims into sending money to someone posing as a friend or relative.

Or they may just turn up at your front door with a collecting box. Don't give. Politely decline and say you choose to make your charitable donations elsewhere. Then visit https://www.charitywatch.org/charity-donating-articles/coronavirus-outbreak for a list of genuine charities accepting coronavirus donations.

**4. Don't believe the face mask hype.** You've seen the videos. You've seen the ads. But according to the US Surgeon General, you're wasting your time.

We're not medical experts here at the Scambusters HQ, so we don't give medical advice. However, Surgeon General Jerome S Adams said on Twitter at the end of February: "Seriously people -- stop buying masks! They're not effective in preventing (the) general public from catching coronavirus."

At the same time, panic-buying of masks is creating a supply shortage for the people who really need them -- medics who have to deal with a whole lot of risks in hospitals and operating theaters.

The CDC says more or less the same thing. At best, the organization points out, masks can only help prevent spread of infection from someone who is already sick.

See this report for an analysis of mask effectiveness: https://thewirecutter.com/blog/face-mask-for-coronavirus/

If you have a mask and want to wear one, the CDC adds, go ahead. It can't do any harm. But it likely won't do you any good either.

**5. Watch out for fake "investment opportunities."** Yes, some scammers are already claiming that the spread of the disease gives investors a chance to make easy money by putting their cash into certain dubious companies.

The US Securities and Exchange Commission (SEC) has issued an investor alert to this effect, warning that fake "research reports" are circulating, making false statements and promoting so-called "penny stocks" or "micro stocks." The crooks want you to buy so they can dump their holdings at a profit.

Read the warning: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus

There's no shortage of reliable news about coronavirus on official sites, like the CDC's. So, look no further if you want to avoid being sucked into this or other pandemic threats.
Reprinted from scambusters.org

# 2020 Security Check

*By George Uliano*

It's that time of the New Year. In January every year I write an article to help you think about your Home, Electronic and Personal Security. In 2019 new advances in electronic locks and Alexa® and Google® Assistant trying to help us with our everyday lives.

**Home Security:**

Make 2020 the year that you invest time and money in securing your home. Do all your doors have deadbolt locks? What about the door going from your garage into your house? ALL doors going into your house should have quality locks and you should know who has keys. You must maintain key control. Does your home have an alarm system? They have come down in price consider getting one installed this year.


**Locks:**

Door locks made big advancements in 2019. Most of these came in the way electronic locks communicate. Physically these locks should be up to the standards of at least a Grade 2 lock. The manufacturers have made it easier to set up and control electronic locks with your smart phone or through your smart assistant. It is now easier to control these locks from a distance through Wi-Fi. Later this year I will be writing an article detailing the new advancements in electronic lock technology.

**Smart Assistants:**

Smart assistants like Alexa® and Google® Assistant are appearing in more devices, such as smart lights, speakers, thermostats, electronic locks, and automobiles. These are just a few, there are many more. I don't think that this trend is going to stop. They are getting better at understanding humans and anticipating what us humans want. I believe that these advancements in smart assistants are good. They will spear head advancements in AI. We just have to make sure that we control and secure smart assistants. They mostly work through Wi-Fi, so make sure that your Wi-Fi is secure with a strong password. Make sure that your routers, modems and switches have been configured with strong passwords that you have provided. If you don't want them listening for their wake command, you can always shut them off. They all have an on/off button.

Make sure that you all travel safe, especially if you go out of the United States. Always leave your itinerary with someone back home, along with copies of your passport and drivers license. Buy travel insurance that can help pay for any medical emergencies or emergency transport back home. And finally, be aware of where you are, if your gut tells you not to go somewhere, don't go.

George Uliano is a security professional with years of law enforcement and security experience. He earned a Bachelors Degree in Criminal Justice and Business graduating with honors. George holds three U.S. patents on different locking principles. This combination gives George and His Company Locking Systems International Inc the unique ability to provide its customers with the correct security at an affordable price.

Article Source: https://EzineArticles.com/expert/George_Uliano/1500014

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

# 7 Reasons to Hire a Good Locksmith

*By Shalini M*

Today, security is of paramount importance whether it's home or office. The reason is that both places contain valuable items that must be secured. Adding a quality security system is one way to protect your premises against burglars. For this purpose, we suggest that you hire the services of a good locksmith. In this article, we are going to take a look at some solid reasons to hire a good locksmith.


**1. They Are Trained**

If you hire a reliable locksmith, you can enjoy a guaranteed service. Typically, these professionals are qualified and trained. Therefore, they can work on different types of locks. They own the right set of tools in order to fix locking issues. It's recommended that you don't work on a lock yourself as you may end up damaging the locking system.

**2. They are Available 24/7**

Professional locksmiths are almost always available. Therefore, they can come to your rescue even if you have an emergency. For instance, if you lose or misplace your keys, you can give a call to them and they will be with you in a jiffy. So, you can rest assured that your problem will be taken care of.

**3. They are Insured**

Most residential and commercial locksmiths are trained and insured. Therefore, they are responsible for the loss that may occur during the work. Their services are quite reliable. So, you can rest assured that they will be there to give you all the help you need.

**4. They offer Reliable Emergency Services**

If you get locked out of your car, home or office, they can come to you on a call. In an emergency, these professionals are reliable and get to your place straight away regardless of the time of day or night.

**5. They Care about their Reputation**

Good professionals are careful enough to develop their reputation and offer the highest quality of services for all their customers. All of them know very well that a bad service will result in unhappy customers, which may ruin their career. Many of them offer a warranty on their service. Therefore, if your security system stops working within the warranty period, they can replace or repair the locks for free.

**6. They have the Right set of Tools**

Most lock problems can be fixed easily. However, some of them are quite complicated and may require the services of an expert. Professionals have all the devices and tools that you need to do this type of jobs in a professional manner. So, in an emergency, you don't need to break your lock or window in order to get inside.

**7. They know the Importance of Security**

If you have trust issues with these pros, know that they have up-to-date security locks for your business and home. Usually, they know a lot about the most recent technologies used in the field. They can give you advice on the highest quality locking system for your home.

In short, if you are looking for a good locksmith, we suggest that you check out Locksmiths365 for a good locksmith Dublin.

Hiring the services of a good locksmith Dublin is a great idea if you want to secure your home or office.

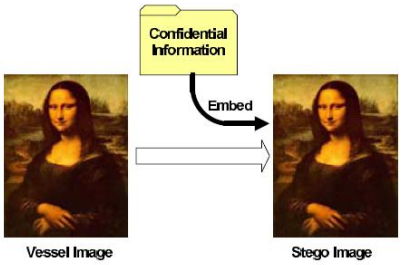
Article Source: https://EzineArticles.com/expert/Shalini_M/2609777

# Hiding in Plain Sight

Don't let the word "stenography" make you think the term has nothing to do with you. Maybe it does.

Yes, it's computer-speak, but what it does is simple. It's a seemingly innocent payload that controls malware that's already been installed on your computer. The best way to deal with it is to render it useless by not letting the malware onto your PC in the first place, as we report in this week's issue.

Let's get started...




**Steganography: Hiding in Plain Sight -- The Threat You've Never Heard Of**

It sounds like a scientific or technical term, which it is, but steganography can actually be a sinister piece of computer-speak that could land you in trouble.

In very simple terms, steganography is a trick that involves hiding one file inside another. More broadly, it refers to any type of information that's hidden inside something that's genuine and innocent looking. For example, in the world of espionage, privacy, and secrecy, it can refer to the use of a hidden coded message inside a piece of normal looking text or art.

It can have a perfectly legitimate security role, for example, by hiding information that identifies a copyrighted document. There are multiple tools available on the Internet for actually using the technique.

But in the scammers' handbook, it's a technique for transferring malware instructions onto an already-infected computer without you seeing or suspecting anything. This way, it can activate malware or simply give it new orders.

**Used in Music Files**

According to the tech site ZDNet, crooks have just started using music files for this purpose. Fortunately, they're not in the standard MP3 digital format most of us download for our listening pleasure. Yet!

Instead, they're in a format known as WAV, which is still in very common use for some types of audio files. In fact, steganography can be used in almost any type of file. It's been around for a number of years and has been, and still is, mainly used by criminals to hide a malicious payload inside picture files (jpeg or .jpg formats).

Its value lies in the way it works.

Most computer security software is set up to identify and block files that are "executable" -- capable of running like any regular computer program or app.

With "stego," as it's called, the file that your computer security software sees is "non-executable," like a jpeg or WAV are. So, it's more likely to be allowed through the security barrier. Only when it's on board your PC does the crooked code emerge to begin its shady business.

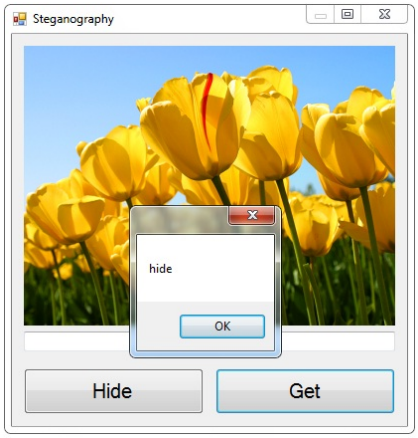
According to security firm Symantec, who recently discovered the trick at work in WAV files, Russian crooks are using it to pass on information or instructions to computers that have already been infected with a virus. Another security organization, Cylance, found evidence just a couple of weeks ago that scammers using botnets (networks of virus-infected PCs) have jumped in on the act.

In this case, they seem to be linked with crypto-mining in which victims' computers are being used to search for virtual currencies, like Bitcoin. (See our report on cryptojacking for more on this -- https://scambusters.org/cryptojacking.html)

**Make It Useless**

In the case of computer malware, you don't need to know how steganography works, but you do need to know how you can best try to beat it. You probably can't stop it,

unless you're a forensic scientist, but you can make it useless.




The first thing to know is that potentially any file you download may have been "steganographed," so you should only download items from sites or people you know and trust.

Most importantly however, as the recent discoveries show, these malicious files are targeted at computers that have already been infected by malware. So, make sure you're malware-free by installing good security software and keeping it up to date.

It's not immediately clear if security software can detect an innocent, non-executable file that's carrying a malicious payload. Probably not. So, it's more important that there's nothing for it to do when it arrives.

ZDNet says: "A proper way of dealing with steganography is... not dealing with it at all. Since stego is only used as a data transfer method, companies should be focusing on detecting the point of entry/infection of the malware that abuses steganography, or the execution of the unauthorized code spawned by the stego-laced files."

The practice of steganography is actually very complex, which explains why it has not been in widespread use in the past. But that's all about to change, as malware writers develop their expertise.
Reprinted from scambusters.org