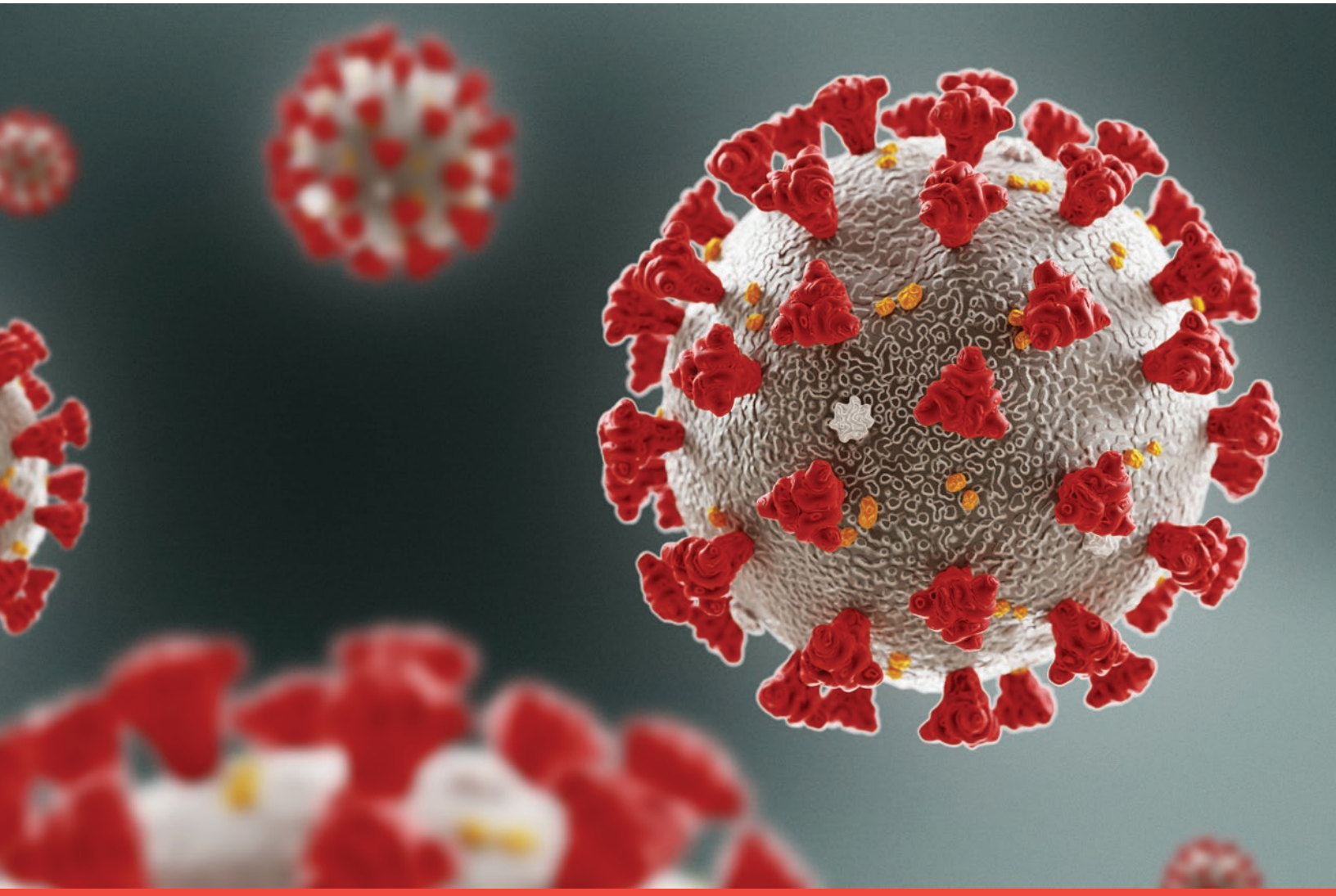
NINJIO



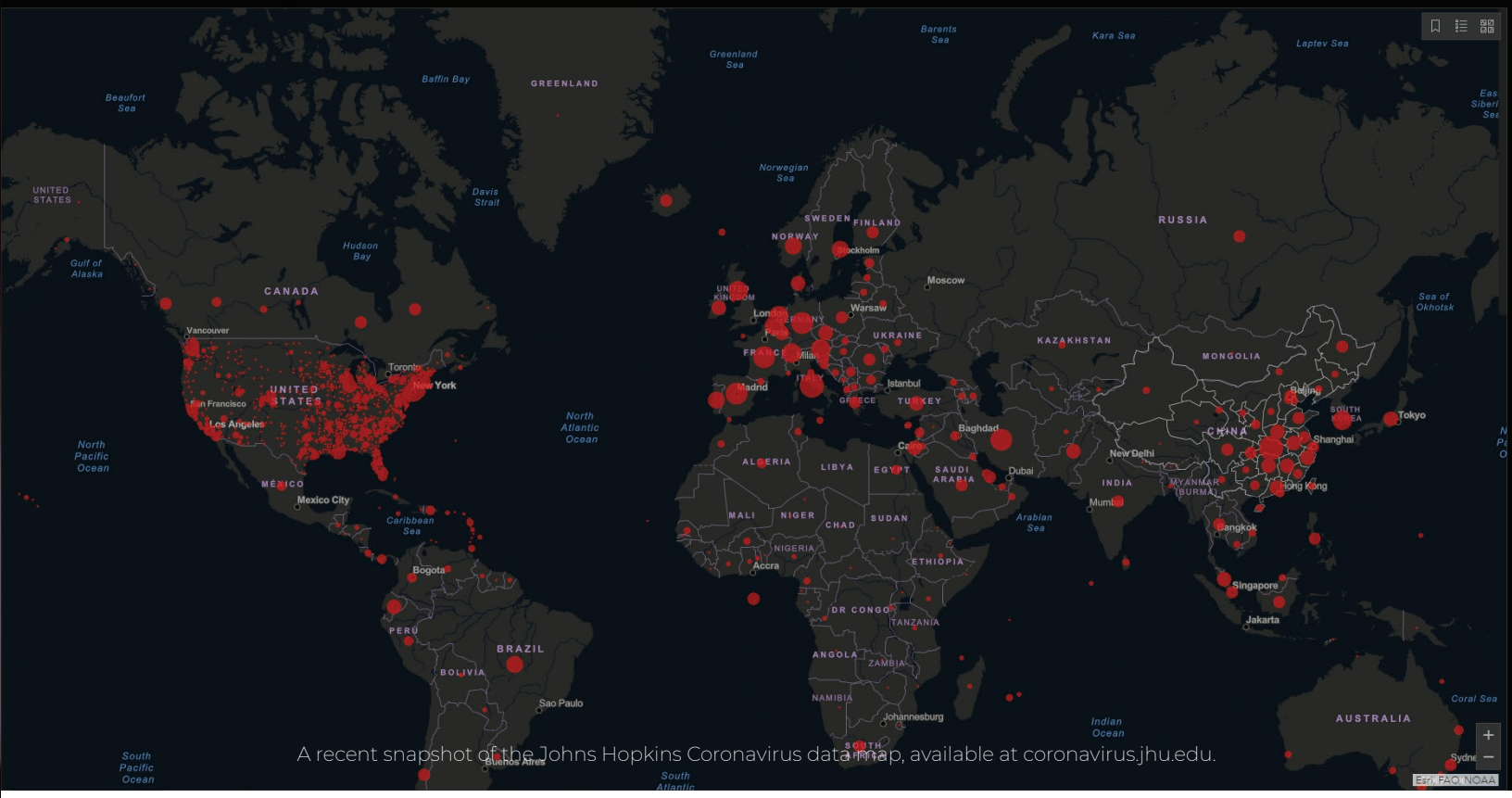
TOP 5
CORONAVIRUS SCAMS

A cybersecurity report on the most pervasive COVID-19 related scams.

One of the reasons NINJIO content is so successful at capturing and holding employees' attention is its relevance – we release new episodes every month that keep users updated on the latest cyberthreats that could harm them, their companies, and their families. As part of our ongoing effort to keep our partners and customers on the cutting edge of cybersecurity awareness, we wanted to inform you about an alarming new development: how hackers are exploiting the Coronavirus pandemic to send their own destructive viruses out into the world.

As millions of people self-quarantine and get accustomed to working from home (often for the first time), they're especially susceptible to cyberattacks. There are many reasons why this is the case, from the use of personal devices that haven't been updated with the latest security software to an explosion of seemingly lucrative offers of remote work that are actually scams. As is so often the case with cybersecurity, the majority of these attacks can be thwarted by educated people using good judgment and knowing what to look for.

That's why we created this report to expose the top five Coronavirus scams and cyberthreats. At a time when you've already taken drastic measures to protect your loved ones and fight back against this pandemic, the last thing you need is to be hacked. Read on to learn how you can prevent that from happening.



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

#1 Coronavirus malware map

One of the go-to resources for anyone who has been tracking the Coronavirus outbreak is an interactive map managed by Johns Hopkins University that provides real-time updates on the spread of the disease. But cybercriminals are now using a fake map to manipulate victims into downloading malware capable of stealing their passwords.

The malware is embedded in a file that has to be downloaded before it can infect the victim's computer. And while the victim has to have Java installed for the infiltration to work, cybersecurity analyst Brian Krebs reports that the seller (who was advertising the malware on a Russian hacker forum) claims it will even work on updated versions of the software. This is a reminder that clever social engineering can help hackers get around digital protections.

TAKE ACTION:

Users can avoid falling victim to this cyberattack by refusing to click on suspicious links or attachments – particularly if they're offering access to data or information that doesn't require any special download to access. There are countless resources for anyone who's interested in staying up to date on Coronavirus, such as the real map on the Johns Hopkins website, The New York Times' daily tracker, and information provided by the Centers for Disease Control and Prevention (CDC). All of these resources are readily accessible online, so there's no reason to risk downloading a map or anything else.

#2 Fraudulent offers of remote work

While many companies have instructed their employees to work from home until further notice, there are also thousands of workers who are out of work altogether. This means they're on the hunt for new jobs, and given the vast shutdowns and layoffs that are taking place outside their front doors, they're turning to the Internet. While remote work can offer many people a lifeline during this period of isolation and economic contraction, cybercriminals are taking advantage of a desperate situation to manipulate and defraud people.

For example, a group of hackers launched a fake nonprofit called the Vasty Health Care Foundation, which tricks job seekers into thinking they've been hired by a nonprofit that's working to help people affected by Coronavirus. In reality, these victims are being used as "money mules" – unwitting intermediaries who help cybercriminals launder stolen money. The hackers will tell victims that a "donation" needs to be processed, so they'll transfer money and ask that it be converted into Bitcoin.

Of course, not all fraudulent work offers are money mule schemes – many are just a way to gain access to sensitive information such as Social Security numbers. These are all reasons why job seekers should work with established companies whenever possible and do their homework on any potential employer – are there reviews on sites like Glassdoor? Is there media coverage you can reference? Have you spoken to anyone at the company over the phone? Did the interview process seem rushed? Do the terms sound too good to be true?

TAKE ACTION:

If you're in search of remote work (especially for the first time), these are all questions you should be asking. You should be even more wary if you're asked to move money around (particularly when cryptocurrency transfers are involved) or if you're asked for sensitive personal information like your SSN and bank account number.

#3 Fear phishing (fake governement alerts)

Cybercriminals have always preyed on the fear of their victims – they use threats and frightening language to coerce people into doing what they say. This is why one of the fastest-growing scams is a fake phone call from the Social Security Administration that convinces victims their SSNs have been compromised or used in criminal activity. Hackers then demand money or "verification" of the SSN, which allows them to steal both. In 2018 alone, 35,000 people were hit with this scam and they lost $10 million.

It's no surprise that cybercriminals are taking full advantage of the fear surrounding Coronavirus. Fake emails from the CDC, the WHO, and other major federal and international agencies are circulating with subject headings like "COVID-19 – Now Airborne, Increased Community Transmission" and offering downloadable information on "little measures that can save you." There are also emails that target people who are more conspiratorial, which claim Coronavirus is a "weapon" designed to "control the citizens of the world." These hackers offer access to information about a fake secret vaccine.

The cybercriminals who create schemes like these use a wide range of hacking tools like keyloggers that can steal credentials and sensitive personal information. Proofpoint researchers report that they've seen "fake Office 365, Adobe, and DocuSign sites" that convince people they're working with legitimate documents. And as with many of the Social Security scams (in which the Social Security Administration's real number appears on caller ID), these hackers are able to imitate legitimate email addresses from organizations like the CDC.

TAKE ACTION:

This is why you should always check the email headers, hover your cursor over links to see where they actually lead, and be extremely suspicious of alarmist messages coming from government agencies that are asking you to do something immediately. Instead, check the alerts on real websites and call the agencies if you have any questions.

#4 How hackers exploit our desire to help

Just as cybercriminals know how to manipulate their victims on the basis of fear, they also know how to take advantage of generosity. The aforementioned Vasty Health Care Foundation scheme told job seekers that the sham organization helps "hospitals from underdeveloped countries to support the highest level health care through the funding of vital medical equipment, research, education, and the provision of items that impact comfort and care."

The hackers clearly assumed that people would be more interested in the fake job posting if they thought it was an opportunity to help people affected by Coronavirus. This is a realization many other cybercriminals have made as well, but they're soliciting money directly. To take just one example: Kaspersky Lab reports that a fraudulent email purportedly sent by the CDC asks recipients to donate to help establish an "incident management system to coordinate a domestic and international public health response" to the pandemic.

While most people will immediately recognize that a federal agency would never send an email soliciting private donations – much less to a Bitcoin account – other cybercriminals are savvier. The Vasty Health Care Foundation website, for instance, uses a template based on a real charity (globalgiving.org) to convince visitors of its legitimacy. The FTC expects the number of phony Coronavirus charities to spike in the coming weeks, and it points out that "Some scammers use names that sound a lot like the names of real charities."

TAKE ACTION:

A recent press release by the office of Georgia's Secretary of State addresses the uptick in counterfeit Coronavirus charities and points out that "awareness is the first line of defense." This is NINJIO's core message, and it's more applicable than ever in the midst of a pandemic. If you want to help Coronavirus victims, visit the websites of well-known charities directly, never enter payment information in response to a solicitation email, and use resources such as GiveWell (which is conducting research on how to mitigate the effects of Coronavirus) and the Better Business Bureau to determine which charities are the most effective.

#5 Hackers are exploiting economic relief effort

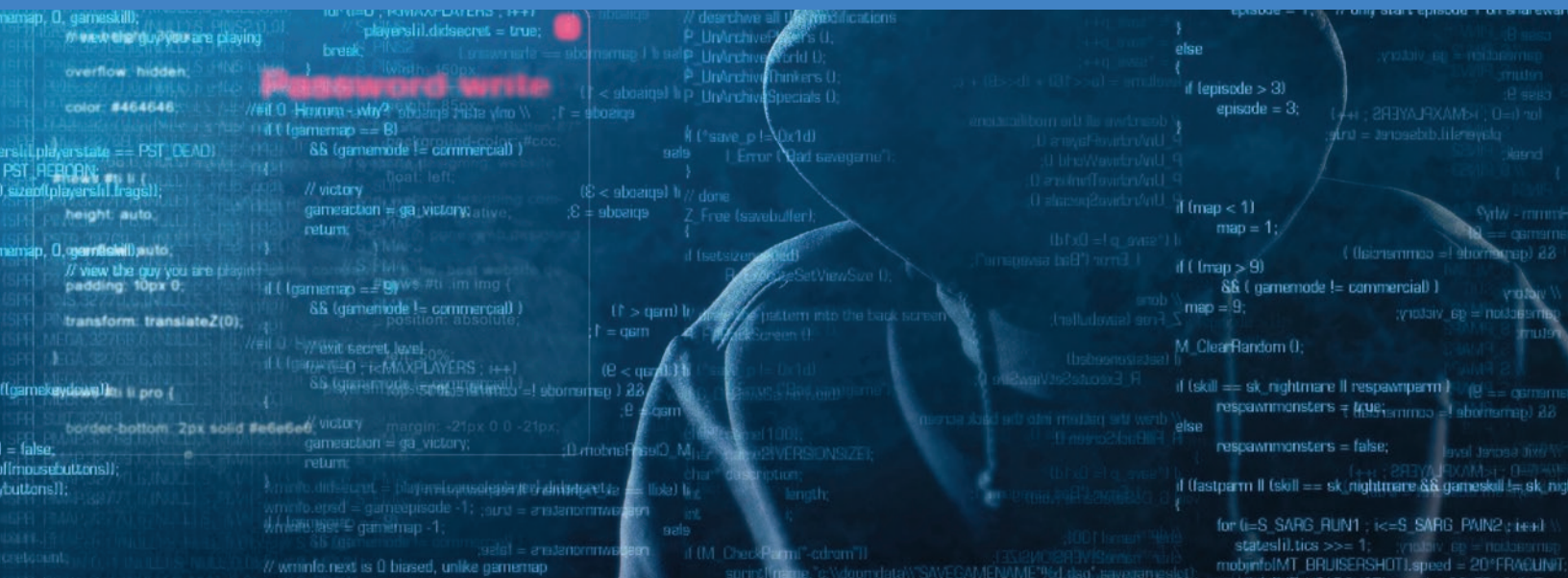
The economic impact of Coronavirus has been immense – the stock market saw its worst single-day drop since 1987 and workers are suffering from an explosion of layoffs. Governments are taking immediate action to stave off a potential recession – for example, the United States is developing a $1 trillion economic stabilization plan that would provide every American adult with a $1,000 check.

This provides even more fertile ground for cybercriminals who are doing everything they can to take advantage of the pandemic. In the coming weeks and months, we shouldn't be surprised if hackers launch a full-on disinformation assault, which will include emails, text messages, phone calls, and just about any other channel of communication that can be used as an attack vector. Government relief programs offer the perfect pretense for cybercriminals to deceive people and steal their information.

NINJIO recently received a direct report of a fraudulent text message that read: "As of March 18th you can qualify for the hardship program. Would you give us a quick call at [a number is listed here] now please to discuss your options?" These scams aren't limited to the United States, either. Mimecast discovered that an artificial email purportedly from the U.K. government has been circulating to "inform" people about a "new tax refund program for dealing with the Coronavirus outbreak." After being told what their "refund" is, victims are instructed to follow a link labeled "Access your funds now." Then they hand over their financial and tax information.

TAKE ACTION:

You should only provide sensitive information directly through the secure online resources provided by your government. Never click on a link in an email that's asking for money. If you have any questions about measures your government is taking to support unemployed or underemployed workers during the pandemic, reach out on the phone via the relevant agency's official phone number. And pay close attention to media reports on stimulus efforts, which will provide projected timelines and other important information.



At a time when cybercriminals are tirelessly developing schemes like these to leverage the mass fear, uncertainty, and desperation caused by the Coronavirus outbreak, we all have to be just as tireless in our efforts to repel their attacks and protect ourselves. While there are many technological defense mechanisms that can be deployed during the period of quarantine and social distancing – such as updating all your devices, using a VPN, and protecting accounts with multi-factor authentication – your most important cybersecurity resource is your own awareness.

NINJIO is dedicated to working with its clients from across the globe to create safe and secure places to work and live. Particularly during this time of health and economic crisis, it's even more important to secure your digital workspaces at home.

Let us know how we can help: connect@ninjio.com

About NINJIO

NINJIO is a cybersecurity awareness training company that empowers individuals and organizations to become defenders against cyberthreats. It was founded in July 2015 by I.T. services industry leader, Zack Schuler. Today, NINJIO creates content that teaches organizations, employees, and families how not to get hacked. They serve some of the largest companies in the world, and have changed the behavior of hundreds of thousands of people through engaging, emotionally-driven storytelling.