MARCH 20, 2020
BRIAN WINTERFELDT, GRIFFIN BARNETT, FRANCISCO CABRERA
ADVISORY

Beware Coronavirus Related Scams: Practical Tips to Protect Yourself and Loved Ones

The coronavirus pandemic has required millions of people to self-quarantine and practice social distancing, resulting in a significant uptick in digital activity. Both work and personal commerce are being conducted through online platforms at an unprecedented rate, and shortages of in-demand products are causing consumers to scour e-commerce platforms for their desired items, often accessing previously unknown sites and brands. Unfortunately, cybercriminals are attempting to capitalize on anxieties over the coronavirus pandemic by rapidly mobilizing vast numbers of potentially-malicious websites and sending scam emails to deceive people into providing their personal information, downloading malicious software, or paying money for goods or services that don’t actually exist. These criminals are also poised to go after business owners’ customers by using their brands to set up elaborate fake charity drives to fool them into believing that they are donating through their preferred company.

People and companies around the world have already fallen prey to these types of scams, with a reported €1 million euros stolen in the United Kingdom alone. The Federal Bureau of Investigation, World Health Organization and the Secret Service have all issued statements warning the public to be careful with emails or websites with information relating to COVID-19. Please find below an overview of common types of fraudulent activities and sites, along with practical tips to avoid becoming a victim of these scams.

Fraudulent websites

One of the more dangerous scams being perpetrated is the registration of domain names that bear the World Health Organization's abbreviations and include content providing alleged advice related to the virus. The following domain names have been reported as being part of a phishing scam seeking to steal Internet users' personal information:

• coronavirusstatus.space

• coronavirus-map.com

• blogcoronacl.canalcero.digital

• coronavirus.zone

• coronavirus-realtime.com

- coronavirus.app
- bgvfr.coronavirusaware.xyz
- coronavirusaware.xyz
- corona-virus.healthcare
- survivecoronavirus.org
- vaccine-coronavirus.com
- coronavirus.cc
- bestcoronavirusprotect.tk
- coronavirusupdate.tk

There has also been a website identified involving a coronavirus map mimicking the legitimate Johns Hopkins' resource. The fake website installs the malware AZORult, which can be used by bad actors to steal credentials and payment information.

The FTC is urging the public to not click on any links from sources they do not already know and trust. Furthermore, the World Health Organization ("WHO") has cautioned the public that it never asks visitors of their official website to visit a link outside www.who.int, nor

does it ask for a username or password to grant access to safety information. It also has clarified that the only call for donations it has issued is the COVID-19 Solidarity Response Fund. Any other appeal for funding or donations that apparently comes from the WHO is a scam.

Phishing emails

“Phishing” is the fraudulent practice of sending emails purporting to be from reputable companies or public institutions in order to deceive individuals into providing sensitive information, such as passwords or credit card numbers. These emails at times can seem very legitimate, sometimes bearing the name of the company in the email address itself or showing an almost exact reproduction of the content usually sent by that company, including legitimate-looking branding elements, signature blocks, and contact information.

There have been reports of email phishing scams using seemingly legitimate email addresses from the Centers for Disease Control and Prevention and the WHO to distribute malware that can steal information from victims’ personal computers. There have also been reports of emails designed to dupe people into donating money for charitable causes relating to COVID-19. Always double-check the source of any emails or requests for donations and only give if you are confident the source is legitimate. For example, when hovering your cursor over links provided in emails, before clicking, please check to see that the link will not take you to an unknown site.

What you can do to protect yourself and your business

The coming months will continue to require individuals and businesses all over the world to make many adjustments to their personal and commercial practices. It is crucial, now more than ever, to exercise extreme caution and vigilance in connection with online activities, and for organizations to take proactive measures to protect themselves and their customers from unscrupulous criminals attempting to exploit this global crisis. It is more important than ever for brand owners and businesses to monitor the online ecosystem for possible consumer scams misusing their intellectual property, including through online domain name, website content, social media, and online marketplace monitoring. It is also critical to ensure proper coordination on consumer outreach and handling of consumer reports of possible phishing or fraud across business units including IT, cybersecurity, legal, marketing, and other relevant teams. Businesses should work with their brand protection vendors and outside counsel to ensure they are prioritizing enforcement targets seeking to leverage the health crisis, in addition to any baseline priorities relating to protecting public health and safety. Unfortunately, much of this work has been impeded by changes to the WHOIS system of domain name registration data, making it easier for cybercriminals to hide from law enforcement and consumer protection agents, as well as evade brand owners looking to directly address scams misusing their brands.

Any US consumer or business can also report any scams you encounter to the Federal Trade Commission (FTC). Review their Complaint Assistance website for more information.

While we have shifted to primarily remote work in light of the pandemic, Winterfeldt IP Group is continuing to operate seamlessly and our team is available to assist you with navigating any ongoing or new intellectual property protection and enforcement priorities. If you have any questions regarding this alert or wish to discuss these matters in more detail, please contact any of the following Winterfeldt IP Group team members:

Brian Winterfeldt, brian@winterfeldt.law, 202-903-4422

Griffin Barnett, griffin@winterfeldt.law, 202-759-5836