



Get the latest on our social pages:



CONTACT:

Frank Scafidi

916.207.0154

fscafidi@nicb.org

Brooke Kelley

847.544.7085

bkelly@nicb.org

Rachel Dooley

814.419.9757

rdooley@cybercrimesupport.org

NEWS RELEASE

April 8, 2020

www.nicb.org

NICB and Cybercrime Support Network Partner to Warn the Public About COVID-19 Scams

DES PLAINES, III.—The [National Insurance Crime Bureau](#) (NICB) and the [Cybercrime Support Network](#) (CSN) are partnering to educate online users about scams surrounding COVID-19, and what consumers need to watch out for when surfing the web, working online, or e-learning from home.

Additional release resources:

[Cybercrime Support Network Scam Alerts](#)

[NICB ID Theft Brochure](#)

[ID Theft Infographic](#)

[FraudSupport.org](#)

[FBI Urges Vigilance During COVID-19 Pandemic](#)

[FTC: Coronavirus Scams](#)

With a high volume of people now working from home and e-learning, there is the potential for cyber criminals to hack into your computer or online meetings and steal your credit card information, or even your identity. Unfortunately, online thieves are standing by, ready to hack your computer and steal your information, especially when you are most vulnerable. Our partnership is aimed at warning consumers to take appropriate security measures to protect your personal information and take every step necessary to protect yourself from becoming a victim of a cyber-attack during these times of uncertainty.

It takes a concerted team effort to fight back against insurance criminals. No individual organization or agency has the resources to single handedly stop these criminals. But by

combining the resources and expertise of insurers, law enforcement agencies, state fraud bureaus, partners like CSN and NICB, insurance fraud can be detected, deterred and stopped—helping to protect all our pocketbooks.

“It all starts with educating yourself about the scams that are happening surrounding the virus, and if it sounds too good to be true it probably is,” said NICB Chief Operating Officer Jim Schweitzer. “As the lockdown continues, the fraudsters will utilize the phone and the internet to try to alleviate your fear and anxiety by promising anything that will cause you to trust them with your sensitive information.”

CSN is here to assist individual and small business victims find the help they need, including referrals to appropriate law enforcement agencies when necessary.

If you believe you have been victimized by one of these online coronavirus scams, first notify your bank or financial institution about the theft of your personal data. Be sure to run a [credit report](#) and monitor for any unusual activity. If you notice a change, freeze your credit with Equifax, Experian, or TransUnion. To learn more about how you can report, recover, and reinforce after a cybersecurity breach, visit FraudSupport’s SSN identity theft [resource page](#).

“Cybercriminals prey on fear. As the pandemic progresses, we can expect to see more and more scams,” said CSN Founder and CEO Kristin Judge. “It is crucial that we provide victims of these scams with the resources they need to report and recover from the incident, then teach them ways to reinforce their cybersecurity. Doing so provides survivors of these crimes with the tools to be confident and empowered when navigating online.”

Online Tips:

- Only disclose information online when the website is secure.
- Before revealing any information – online, over the phone, or in-person – verify the identity of the person and organization then ask how it will be used.
- Carefully review all monthly credit card statements and check for unauthorized use.
- Never send gift cards, wire money or send a check to a stranger. If someone is pressuring you to pay with a gift card, it is a scam.
- If someone claims to be from a federal agency, call the office to confirm.

We encourage you to educate yourself about these online COVID-19 scams and help turn the tables on the thieves looking to steal your information.

In an effort to get the word out about the latest virus information and what’s happening in our states from a fraud perspective, we have published the [COVID-19 NICB Resource Center](#), which is a comprehensive web page that highlights national and state resources that are available to identify and fight the insurance fraud that is sure to come as a result of this crisis.

You can find that link on our website: www.nicb.org.

REPORT FRAUD: Anyone with information concerning insurance fraud or vehicle theft can report it anonymously by calling toll-free 800.TEL.NICB (800.835.6422) or submitting a [form](#) on our website.

ABOUT THE NATIONAL INSURANCE CRIME BUREAU: Headquartered in Des Plaines, Ill., the NICB is the nation's leading not-for-profit organization exclusively dedicated to preventing, detecting and defeating insurance fraud and vehicle theft through data analytics, investigations, learning and development, government affairs and public affairs. The NICB is supported by more than 1,300 property and casualty insurance companies and self-insured organizations. NICB member companies wrote over \$525 billion in insurance premiums in 2019, or more than 82% of the nation's property/casualty insurance. That includes more than 95% (\$253 billion) of the nation's personal auto insurance. To learn more visit www.nicb.org.

ABOUT CYBERCRIME SUPPORT NETWORK: Cybercrime Support Network (CSN) is a public-private, nonprofit collaboration created to be the voice of cybercrime victims. CSN created FraudSupport.org to provide assistance to both individual and small business cybercrime victims. FraudSupport.org will lead cybercrime victims through the Report, Recover and Reinforce process after an incident occurs.

Follow us on [Twitter](#), [Facebook](#), and [YouTube](#)
For more information, please visit: Cybercrimesupport.org

###