



New Hampshire Information & Analysis Center

COVID-19 Daily Report

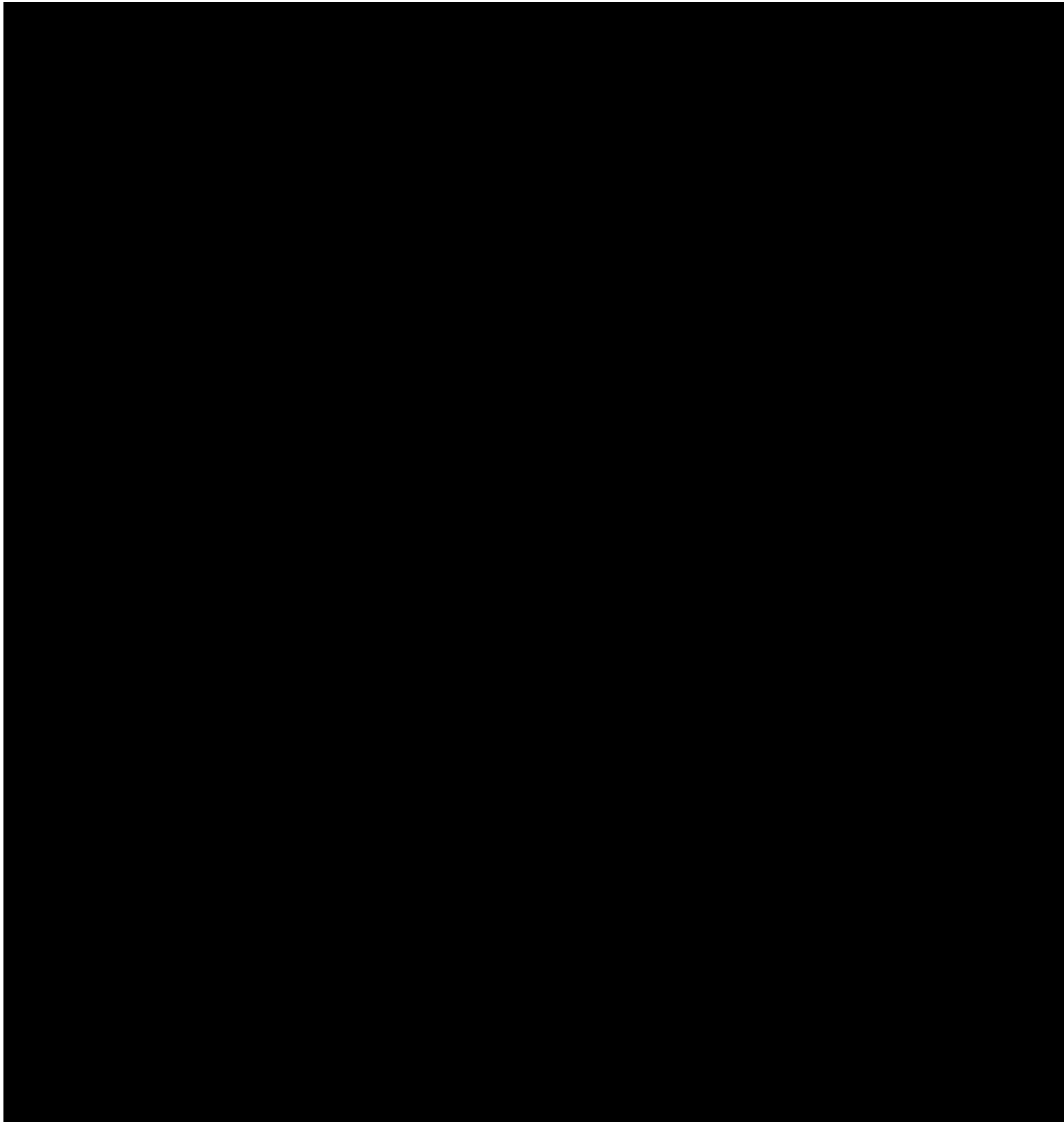
22 April 2020

Bulletin #2020-4118

SINs: NHIAC – 16 | HSEC – 6

(603) 223-3859

NH.IAC@dos.nh.gov



New Hampshire Information & Analysis Center – COVID-19 Daily Report

(U) COVID-19 Related Activities

(U) OUT OF STATE

TLP:GREEN Not to be shared with the public or media – Nationwide - *Indicators of Fraudulent 3M Personal Protective Equipment* - The Federal Bureau of Investigation (FBI) Minneapolis Division, in coordination with the Office of Private Sector (OPS), Criminal Investigative Division (CID), and 3M, prepared this LIR to make the Healthcare and Public Health Sectors aware of indicators related to fraudulent sales solicitation of 3M Personal Protective Equipment (PPE), or indicators of counterfeit 3M PPE, including N95 respirators.

- **Source:** Federal Bureau of Investigation (FBI) Minneapolis Division – Liaison Information Report (LIR) [🔗](#)

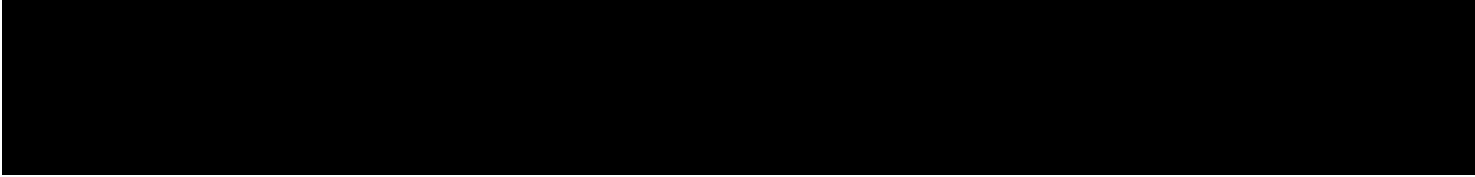
(U) Nationwide - *U.S. SECRET SERVICE IN PARTNERSHIP WITH THE U.S. DEPARTMENT OF THE TREASURY LAUNCH - KNOW YOUR U.S. TREASURY CHECK CAMPAIGN* - The Secret Service in partnership with the U.S. Department of the Treasury is leading the charge to bring awareness to citizens, retailers and financial institutions on how to protect themselves from becoming a victim of easy to detect counterfeit U.S. Treasury Checks. According to the Internal Revenue Service (IRS), paper U.S. Treasury checks from the \$2 trillion dollar Coronavirus Aid, Relief and Economic Security Act (CARES Act) will be mailed and issued to millions of Americans beginning late April, 2020. With the implementation of the CARES Act, comes opportunities for criminal activity, like check fraud. The Secret Service and the U.S. Department of the Treasury want to inform citizens and consumers nationwide on ways to protect themselves during these times. This announcement contains information that consumers and financial institutions can use to identify counterfeit U.S Treasury checks by knowing what to look for and where to look.

- United States Secret Service – Press Release [🔗](#)

TLP:WHITE – Nationwide - *COVID-19 Email Phishing Against US Healthcare Providers* - Following a global increase in malicious cyber activity exploiting fear derived from the COVID-19 pandemic, the Federal Bureau of Investigation (FBI) was notified of targeted email phishing attempts against US-based medical providers. These attempts leveraged email subject lines and content related to COVID-19 to distribute malicious attachments, which exploited Microsoft Word Document files, 7-zip compressed files, Microsoft Visual Basic Script, Java, and Microsoft Executables. The FBI is providing indicators of compromise related to these phishing attempts to assist network defenders in protecting their environments. Additionally, the FBI is providing the attached list of hashes related to additional COVID-19 phishing.

- The New Hampshire Information & Analysis Center (NHIAC) would like to draw attention to the second page of this product for more detailed description on the email senders, email subjects, attachment file names, and hash values.
- **Source:** Federal Bureau of Investigation (FBI) – Cyber Division – FBI Flash [🔗](#)

New Hampshire Information & Analysis Center – COVID-19 Daily Report



(U) Nationwide – *Online Extortion Scams Increasing during the COVID-19 Crisis* - The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) has seen an increase in reports of online extortion scams during the current "stay-at-home" orders due to the COVID-19 crisis. Because large swaths of the population are staying at home and likely using the computer more than usual, scammers may use this opportunity to find new victims and pressure them into sending money. The scammers are sending e-mails threatening to release sexually explicit photos or personally compromising videos to the individual's contacts if they do not pay. While there are many variations of these online extortion attempts, they often share certain commonalities.

- Source: Federal Bureau of Investigation (FBI) – Internet Crime Complaint Center (IC3) – Public Service Announcement [🔗](#)
- 