FBI Urges Vigilance During COVID-19 Pandemic

The FBI urges the public to remain vigilant for fraud schemes and other unlawful activity, including:

	Civil Rights	Child Exploitation	Cyber Crimes
How it Occurs	Hate crimes or bias-motivated harassment.	With schools closed, sexual predators can take advantage of children's increased time online.	Cyber actors taking advantage of virtual vulnerabilities related to telework, communication systems, and software.
Ways to Protect Yourself	• If in physical danger, retreat to safe location. • If a telephone threat, remain calm. Signal others nearby to call 911. • If possible, preserve any evidence —emails, notes, etc. • Write down verbal threats.	• Discuss Internet safety with children. • Review and approve games and apps before they are downloaded. • Make sure privacy settings are set to the strictest level possible for online gaming systems and electronic devices. • Monitor your children's use of the Internet; keep electronic devices in an open, common room of the house. • Check your children's profiles and what they post online. • If possible, preserve any evidence — emails, notes, etc.	• Verify web address links; manually type in browser; check domain name spelling. (i.e., do government websites end in .gov?) • Use trusted telework software vendors; use extra due diligence when vendor is foreign-sourced. • Restrict online meeting, conference call, or virtual classroom access. • Use tools that block suspected phishing emails or allow users to report and quarantine them. • Research before contributing to charities or crowdfunding, purchasing products, or providing personal information. • Don't provide usernames, passwords, birth dates, social security numbers, financial data, etc. via email. • Don't use unsecured Wi-Fi to access sensitive information. • Don't reuse passwords for multiple accounts. • Don't use remote desktop sharing. • Don't provide exact details on child's user profile (i.e., use initials vs. full name, avoid exact date of birth or photos.) • Don't open email attachments or links from unfamiliar senders. • Be wary of websites or apps claiming to track COVID-19 cases; malicious websites can infect or lock devices for ransom.
Where to Get More Information	• https://www.fbi.gov/investigate/civil-rights/hate-crimes	• https://www.fbi.gov/news/pressrel/press-releases/school-closings-due-to-covid-19-present-potential-for-increased-risk-of-child-exploitation	• https://www.ic3.gov/media/2020/200401.aspx • www.ic3.gov/media/2020/200320.aspx
How to Report	• Once safe, call 911. • Contact local FBI office; ask to submit hate crime complaint to Civil Rights squad or submit a tip at https://tips.fbi.gov/	• Contact local law enforcement. • Contact local FBI office or submit a tip at https://tips.fbi.gov/ • File report with National Center for Missing & Exploited Children (NCMEC) at 1-800-843-5678 or at www.cybertipline.org	• If transfer of funds occurred, immediately contact your financial institution to request recall of funds; contact your employer to report irregularities with payroll deposits. • As soon as possible, file complaint with FBI's Internet Crime Complaint Center at www.ic3.gov

FBI Urges Vigilance During COVID-19 Pandemic continued

The FBI urges the public to remain vigilant for fraud schemes and other unlawful activity, including:

	Business Email Compromise	Frauds and Swindles	Price Gouging and Hoarding
How it Occurs	Cyber criminals spoofing websites, sending spearfishing emails, and employing malware.	Criminals using stimulus checks as a ruse to obtain information; sale of fraudulent cures and medicines; seller purporting to have PPE but does not deliver product after payment.	Bad actors who charge extraordinary prices for medical supplies or who amass critical supplies either far beyond what they could use or for the purpose of profiteering.
Ways to Protect Yourself	• Check last-minute changes in wiring instructions or recipient account information. • Verify vendor information via the recipient's contact information on file — not the number in the email. • Verify sender email addresses, especially when using a mobile or handheld device (i.e., does sender's email address match who it is from.) • Change default settings to unique passwords on routers and smart devices. • Install anti-virus software on desktops, laptops, and mobile devices; apply routine security updates; regularly update web browsers, plugins, and document readers.	• Understand there is currently no cure for COVID-19; any claims selling one are fraud. • The government is **not** sending emails or calling to confirm personal information; IRS first form of communication is mail. • Watch out for emails or persons going door to door claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. • Don't provide usernames, passwords, birthdates, social security numbers, financial data, etc. via email or to robocalls. • Verify web address links; manually type in browser; check domain name spelling? (i.e., do government websites end in .gov?)	• Recognize health and medical supply items designated by Secretary of Health and Human Services that must not be hoarded or sold for exorbitant prices including: personal protective equipment (PPE)—masks, shields, gloves, etc.; respirators; ventilators; drug products; sterilization services; disinfecting devices; medical gowns or apparel.
Where to Get More Information	• https://www.ic3.gov/media/2020/200401.aspx	• www.ic3.gov/media/2020/200320.aspx • https://www.justice.gov/coronavirus • https://www.treasury.gov/tigta/coronavirus.shtml • The best sources for authoritative information on COVID-19 are www.cdc.gov and www.coronavirus.gov.	• https://www.justice.gov/coronavirus/combattingpricegouginghoarding
How to Report	• If transfer of funds occurred, immediately contact your financial institution to request recall of funds; contact your employer to report irregularities with payroll deposits. • File BEC and/or email account compromise (EAC) complaints at BEC.IC3.gov	• If transfer of funds occurred, immediately contact your financial institution to request recall of funds; contact your employer to report irregularities with payroll deposits. • As soon as possible, file complaint with FBI's Internet Crime Complaint Center at www.ic3.gov. • Report IRS-related coronavirus scams at https://www.treasury.gov/tigta/contact_report_covid.shtml	• Report to the Department of Justice's National Center for Disaster Fraud by calling the National Hotline at (866) 720-5721 or by email at https://www.justice.gov/disaster-fraud/webform/ncdf-disaster-complaint-form

FBI Urges Vigilance During COVID-19 Pandemic continued

The FBI urges the public to remain vigilant for fraud schemes and other unlawful activity, including:

	Health Care Fraud Schemes	Money Laundering Facilitation	Intellectual Property Rights
How it Occurs	Decreased requirements for ordered lab tests and growing telemedicine is increasing opportunities for providers to fraudulently bill Medicare, Medicaid, and private insurers.	Fraudsters use unsuspecting individuals to move illicit proceeds through fund transfers or physical cash in order to make proceeds appear legitimate rather than having come from criminal activity. Criminals will target you through online job application schemes or dating apps/websites.	Products that do not meet approved standards for protection are counterfeited and passed off as authentic. In addition, Intellectual Property Rights violations include potential theft of technology by non-state actors who seek to rapidly expand manufacturing and production of healthcare supplies, pharmaceuticals, and vaccines.
Ways to Protect Yourself	• Be aware of unsolicited requests for your Medicare information; scammers use this information to submit false medical claims for unrelated, unnecessary, or fictitious services. • Health care workers and insurance company workers should be cognizant of excessive orders for and billing of unnecessary or duplicate tests.	• Do not give your bank account information to anyone via the phone or Internet who you do not know or who contacted you unsolicited. • Do not move money for people you do not know via wire transfer, ACH, mail, or money service. • Be wary of anyone who asks you to move money for them, especially those claiming to be a U.S. citizen abroad or those offering for you to keep a portion of the transfer.	• Consult the CDC website for a list of all NIOSH-approved N95 respirator manufacturers and validate approval and certification numbers: https://www.cdc.gov/niosh/ • If procuring categories of PPE such as gowns, gloves, goggles, and face shields, consult the manufacturer to verify authenticity and availability. • Be wary of repurposed or "off-label" medications.
Where to Get More Information	• https://www.fbi.gov.investigate/white-collar-crime/health-care-fraud	• https://www.fbi.gov/file-repository/money-mule-awareness-booklet.pdf/view • https://www.fbi.gov/news/stories/money-muling-is-illegal-120419 • https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-money-mule-schemes-exploiting-the-covid-19-pandemic	• For information about respirators, consult the CDC National Institute for Safety and Health (NIOSH): https://www.cdc.gov/niosh/npptl/usernotices/counterfeit Resp.html • Websites of PPE manufacturers
How to Report	• Report Medicare fraud to the U.S. Department of Health & Human Services at 1-800-447-8477. • Report Minnesota Medicaid fraud at 1-888-742-7248. • Report personal care attendant fraud or suspicions of elder abuse to your local county. • Contact local FBI office or submit a tip at https://tips.fbi.gov/.	• Report this activity to the FBI's Internet Crime Complaint Center at www.ic3.gov	• Report allegations of counterfeit PPE to HSI: https://eallegations.cbp.gov/Home/allegation • E-mail ICE HSI at: Covid19Fraud@dhs.gov • Contact the National Disaster Fraud Hotline at 1-866-720-5721. • Contact the National Intellectual Property Rights Coordination Center at iprcenter.gov. • Contact the manufacturer whose brand is being counterfeited.