Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**April 20, 2020**

Alert Number

**I-042020-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.
Local Field Office Locations: www.fbi.gov/contact-us/field

# ONLINE EXTORTION SCAMS INCREASING DURING THE COVID-19 CRISIS

The 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 commonalties.

**SCAM COMMONALTIES:**
Online extortion schemes vary, but there are a few common indicators of the scam. The following characteristics are not all-inclusive but should serve as red flags. It is important to remember that scammers adapt their schemes to capitalize on current events such as the COVID-19 pandemic, high-profile breaches, or new trends involving the Internet, all in an attempt to make their scams seem more authentic.

- The online extortion attempt comes as an e-mail from an unknown party and, many times, will be written in broken English with grammatical errors.
- The recipient's personal information is noted in the e-mail or letter to add a higher degree of intimidation to the scam. For example, the recipient's user name or password is provided at the beginning of the e-mail or letter.
- The recipient is accused of visiting adult websites, cheating on a spouse, or being involved in other compromising situations.
- The e-mail or letter includes a statement like, "I had a serious spyware and adware infect your computer," or "I have a recorded video of you" as an explanation of how the information was allegedly gathered.
- The e-mail or letter threatens to send a video or other compromising information to family, friends, coworkers, or social network contacts if a ransom is not paid.
- The e-mail or letter provides a short window to pay, typically 48 hours.
- The recipient is instructed to pay the ransom in Bitcoin, a virtual currency that provides a high degree of anonymity to the transactions.

**TIPS TO PROTECT YOURSELF:**

- Do not open e-mails or attachments from unknown individuals.
- Monitor your bank account statements regularly, and your credit report at least once a year for any unusual activity.
- Do not communicate with unsolicited e-mail senders.
- Do not store sensitive or embarrassing photos or information online or on your mobile devices.
- Use strong passwords and do not use the same password for multiple websites.
- Never provide personal information of any sort via e-mail. Be aware that many e-mails requesting your personal information appear to be legitimate.
- Ensure security settings for social media accounts are activated and set at the highest level of protection.
- Verify the web address of legitimate websites and manually type the address into your browser.

The FBI does not condone the payment of online extortion demands as the funds will facilitate continued criminal activity, including potential organized crime activity and associated violent crimes.

**VICTIM REPORTING:**
If you believe you have been a victim of this scam, reach out to your local FBI field office, and file a complaint with the IC3 at www.ic3.gov. Please provide any relevant information in your complaint, including the online extortion e-mail with header information and Bitcoin address if available.