Consumer Advisory

Bitcoin Blackmail Scam - Spring 2020

Recently, the Consumer Fraud Protection Division of the 18th Judicial District Attorney's Office has fielded increasing numbers of complaints from concerned citizens. Several members of our community have received emails on their personal accounts from unknown sources stating that their computer has been hacked, their webcam is being monitored, and their contact list has been seized. In addition, the scammers state that they have recorded the complainant visiting adult websites and threaten to distribute the video within hours to family and friends unless they deposit $2000.00 in bitcoin into a specified account. These complaints seem to be consistent with similar incidents that are taking place across the state of Colorado and even on a national level. **This is a scam!**

The details and circumstances have been very similar, if not exact, with each complaint. The name of the sender varies. The email subject line may contain a previous or partially-correct email address and password used by the complainant. This leads the recipients to open the email, even though the sender was unknown to them. Most recipients suspect it is scam because of the emails reference non-existent cameras or non-existent social media accounts, but they still are concerned.

Probable Circumstances:

The timing and probable root cause of this particular scam is likely due to one or more recent data breaches of company accounts that exposed email addresses and passwords but no financial information. As a result, scammers may have actual or partial email addresses and passwords, and are placing them in the email messages as "proof" they have hacked the email target's computer. Claims the hacker seized data from an individual's computer or hacked into a webcam are untrue. Data breaches are unfortunate, but they do happen as technology continues to evolve.

Suggested Action:

Stop and set aside your emotional reaction! Do not open any other suspicious emails or attachments. Do not pay anything. Delete the message. Update and change your passwords (regularly chose strong ones).

If you or someone you know receives this email or one similar in nature, please report it to:

- Federal Bureau of Investigation – Internet Crime Complaint Center: **www.ic3.gov**
- Federal Trade Commission: **www.FTC.gov/Complaint**
- Consumer Fraud Protection – 18th Judicial District Colorado: **consumer@da18.state.co.us**

If you receive an email with threats or acts of extortion where the sender is unknown, it appears to be a large-scale or general message, or it may relate to a recently known data breach, start by filing a complaint with the FBI and FTC at the links above. These government agencies have expanded resources to probe further and determine if complaint is a regional or national matter. The more information they receive from a broad population base, the more effective they can be in identifying root sources and suppressing the scammers. Always feel free to contact our office to report the matter. We are here to support you.

Should you receive a threatening email or communication from a known individual or you feel a particular email is a direct personal threat against you, please report the incident to your local law enforcement agency and to our Consumer Fraud Protection Division. You may contact our hotline at (720) 847-8547 or email us at **consumer@da18.state.co.us**.