ERIK NASARENKO
VENTURA COUNTY DISTRICT ATTORNEY
NEWS RELEASE

Follow us @VenturaCountyDA
vcdistrictattorney.com

Contact: Scott Whitney
Title: Chief Investigator
Phone: (805) 477-1614
Email: Scott.Whitney@ventura.org

Approved: SW
Date: November 1, 2024
Release No.: 24-129

District Attorney Warns of New Email Scam

VENTURA, Calif. – In recent weeks, the Ventura County District Attorney's Office has received reports of county residents being targeted by a specific email scam. The scam is unnerving because the email begins by listing the victim's name, phone number, home address, and may even include a photo of the victim's home. The scammers use this tactic to make the victims feel that they have been singled out and to create fear.

The scammers then claim to have hacked into the victim's computer or smartphone and to be actively monitoring the victim's browsing habits and websites visited, with references to "porn websites." The scam email typically threatens, "With just a single click, I can send this filth to all your contacts." The scammers do this to make the victims feel embarrassed and to create a sense of urgency.

The scammers close the email with an extortion attempt. They present two alternatives to the victim. The scammers claim that if the victim "disregards this email" that they will send embarrassing information "to all your contacts." The scammers then offer to "wipe everything clean once you come through with a payment." The payment demand is typically about $2000, payable with "Bitcoins only."

This current scam uses similar tactics to other sextortion scams that threaten to release embarrassing images or videos unless a payment demand is met. This is a widespread scam using boilerplate language and targeting victims throughout the country. The scammers likely obtained the victims' personal identifying information from a large-scale data breach, not by hacking the victims' devices. Images of victims' homes are easily obtained through open-source searches such as Google Street View, Zillow, or other similar websites. The scammers are often located outside the United States.

“It can be very rattling for an unsuspecting victim to receive one of these threatening emails,” said Ventura County District Attorney Erik Nasarenko. “The best defense against these scammers is being aware of their tactics and taking practical steps to avoid becoming a victim.”

Practical steps to protect yourself include:

- Like any other scam, it is important not to reply to the suspects. Communicating with the suspects increases the chances of accidentally disclosing personal information the suspect did not have.
- Never click on attachments or links that come from unknown sources.
- Do not readily share personal identifying information such as your full name, address, or social security number online.
- Use two-factor authentication for all accounts that offer it. This adds an extra layer of security.
- Monitor your online social media, email, and banking accounts for suspicious activity.
- Change your passwords regularly and use a unique password for each account.
- If you paid the extortion, notify your bank or financial institutions. Promptly report any unauthorized transactions so they can block or reverse the payments. Report the crime to your local law enforcement.
- Victims can also report scams to the Internet Crime Complaint Center (IC3.gov). This is a user-friendly, FBI-run website for reporting cyber-enabled crime.