

Tech Tuesday: Building a Digital Defense Against Sextortion Crimes

September 12, 2021

A graphic with a dark blue background featuring a circuit board pattern. In the center, a large, faint, circular seal of the Federal Bureau of Investigation is visible. The text is white and bold. At the top, it says "TECH TUESDAY: Sextortion Crimes". Below this is a bulleted list of five items. At the bottom left is the FBI logo and the text "FBI FEDERAL BUREAU OF INVESTIGATION". At the bottom right is the text "Portland Field Office".

TECH TUESDAY: Sextortion Crimes

- Don't ever send compromising photos or videos of yourself to anyone.
- Turn off devices & webcams when not in use.
- Never open attachments or click on links.
- If you are a victim, report this crime to the FBI or other law enforcement right away.
- Report to www.ic3.gov or tips.fbi.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against sextortion crimes.

The FBI's Internet Crime Complaint Center (IC3) is warning about a large increase in the number of sextortion complaints. Sextortion happens when someone threatens to distribute your private and sensitive material if their demands aren't met. Oftentimes, the fraudster demands additional sexual images, sexual favors, or money – creating financial and emotional distress for the victim.

In just the first seven months of this year, IC3 has received more than 16,000 sextortion complaints. The losses have topped \$8 million. Almost half of these extortion victims were in the 20-39 age group. Victims over the age of 60 years are also prime targets.

Most adult victims report the initial contact with the fraudster is mutual and made using dating websites and apps. For kids, the contacts can come through online games or social media platforms that young people tend to use.

Soon after the initial encounter, the fraudster requests the interaction be moved from the website or app to another messaging platform. The fraudster either threatens that he already possesses embarrassing photos, or he instigates the exchange of sexually explicit material. He often encourages the victim to participate via video chat or to send their own explicit photos.

Immediately after the victim complies, the fraudster blackmails the victim and demands money to prevent the release of the photos or videos on social media. He may also demand more and more images. The fraudster often gains access to the victim's social media accounts or contact information and threatens to send the images to the victim's family and friends.

How to protect yourself:

NEVER send compromising images of yourself to anyone, no matter who they are or who they say they are. Do not open attachments from people you do not know. Links can secretly hack your electronic devices using malware to gain access to your private data, photos, and contacts. There is also malware that can control your web camera and microphone without your knowledge. Turn off your electronic devices and web cameras when not in use.

If you are receiving sextortion threats:

Remember you are not alone as thousands are victimized by this scam. Stop all interaction with the extortionist and do not be embarrassed or afraid to contact law enforcement.

Additional information on sextortion is available here:

Downloadable video: <https://www.fbi.gov/video-repository/newss-what-is-sextortion/view>

Information specific to teens & sextortion:

<https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/sextortion>

If you are the victim of an online fraud, you should report the incident to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.