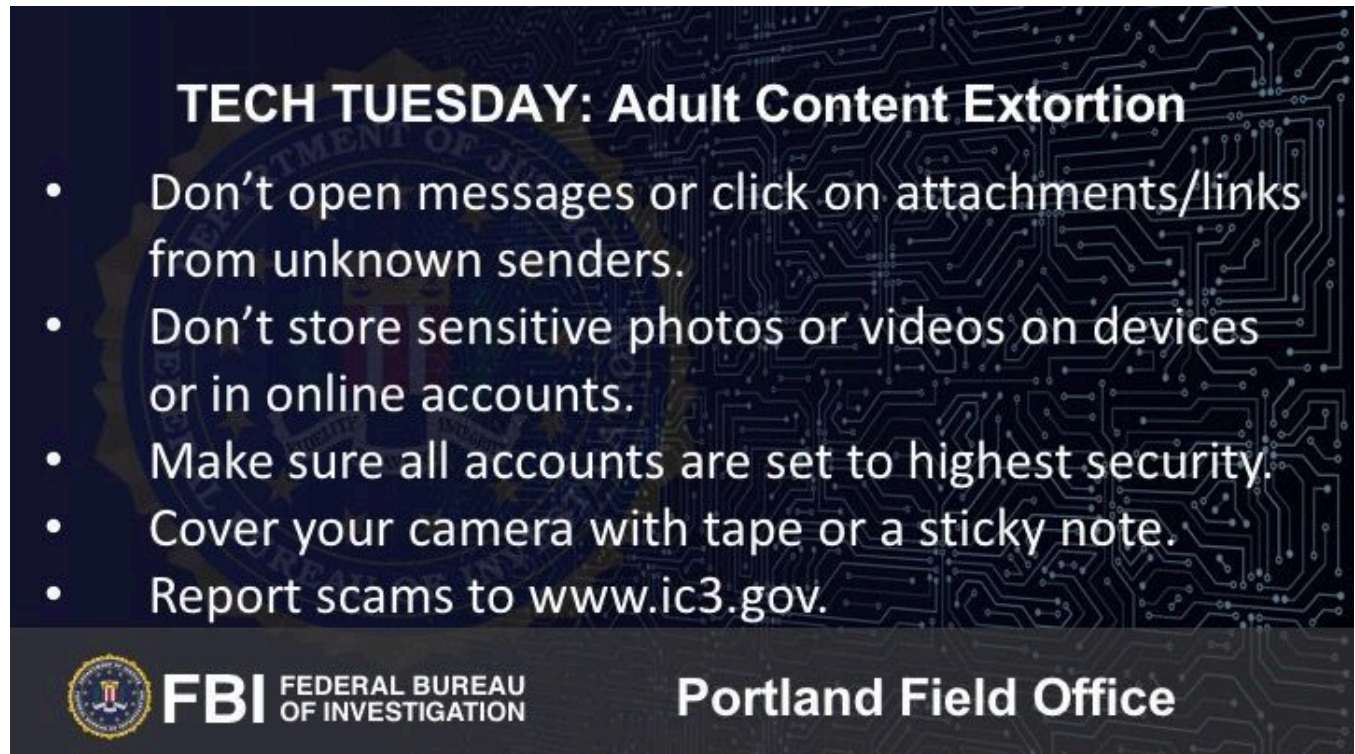


Tech Tuesday: Building a Digital Defense Against Adult Content Extortion

May 25, 2021

A graphic with a dark blue background featuring a circuit board pattern. In the center is a large, faint, circular seal of the Federal Bureau of Investigation. Overlaid on this is the title "TECH TUESDAY: Adult Content Extortion" in bold white text. Below the title 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" in bold white font.

TECH TUESDAY: Adult Content Extortion

- Don't open messages or click on attachments/links from unknown senders.
- Don't store sensitive photos or videos on devices or in online accounts.
- Make sure all accounts are set to highest security.
- Cover your camera with tape or a sticky note.
- Report scams to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against adult content extortion schemes.

Extortion schemes are as old as time, but in recent years we've seen a number of scams in which the fraudster says he has photos or videos of the victim in compromising positions. Usually the victim receives an email with his or her name listed and maybe some personal details... just enough to make it seem as though the bad guy really has something on you. He demands payment, often within 48 hours, or he threatens to release the images he allegedly has of you to your friends and family.

Well lately, we've been seeing a number of extortion complaints from Oregonians coming in through the FBI's Internet Crime Complaint Center, and these complaints have a few new twists. The fraudster attaches a document or photo showing what, he says, is his proof. That attachment is likely loaded with malware that will infect your device if you click on it.

This new scammer also threatens that he will block your access to your device and social media accounts – much like a ransomware attack – if you choose to ignore his warning. And, while bad spelling and syntax are common, these particular messages come with a distinctly English take on things. In particular, the fraudster is using common British words or phrases to describe sex acts as opposed to what you might hear more commonly in the U.S.

Here are some ways to protect yourself:

Don't open emails or attachments from unknown people, and don't communicate with those who send unsolicited messages.

Don't store sensitive or embarrassing photos or information online or on your mobile devices.

Use strong passwords and don't use the same password for multiple websites.

Never provide personal information of any sort via email. Be aware that many fraudulent emails requesting your personal information appear to be legitimate.

Make sure you have activated the security settings for social media accounts and that they are set at the highest level of protection.

Cover up your camera. Simple piece of colored tape or a sticky note will do the trick.

Note: the FBI does not condone the payment of online extortion demands as the funds will facilitate continued criminal activity.

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.