Virtually Held for Ransom

Scammers have moved beyond phony sweepstakes and phishing profiles. They are now into scare tactics in a ruse intended to rob you of your money by blackmail.

Email extortion scams and webcam blackmails are circulating, threatening recipients with the release of their sensitive information if money isn't paid immediately. These scammers send emails stating they are reading your emails, monitoring your internet usage, or videotaping you via a webcam and now you must pay to retain your privacy.

They email with the From: address the same as the To: address, so it looks as though your device sent the email. This simple, but frightening, tactic creates the illusion that they have control of your account. They don't. This email is actually a spam email sent to thousands of email addresses in hopes of tricking at least one person.

What to Look For

These extortion email scams are a bluff, but they are very effective at scaring you into immediate action—action that you don't need to take. There are telltale signs that the email is a hoax:

· The email includes a password you use online or one you used in the past.
· The email is vague and doesn't include any specific website you visited.
· The threat is poorly worded with grammatical and spelling errors.
· You are given a short deadline to respond, like a day or two.

Often, your antivirus blocks these emails, diverting them to your email Junk folder. The cybersecurity company, Symantec, recently reported blocking 289 million extortion emails in the first five months of 2019. This email scam is low cost/high return for these tricksters and they only need one hit to make it lucrative for them. The FBI's   Internet Crime Complaint Center (IC3) documented 43,101 cases of online extortion in 2019.

Resources

· Report extortion attempts to an FBI field office in your area or to the IC3 .
· Check if your email address was involved in a website data breach on the website Have I Been Pwned which tracks website data breaches and lets you check if your email address was compromised.