A viewer forwarded me an email she received this week that frightened her. The email was threatening and promised to extort her out of about $1,500. It's a scam that rears its ugly head ever few years (the last time I mentioned it was 2020) because it works. I'm looking into the scam and how it works and an easy way to help you answer the question: "is this a scam?"

TRT 128
STD OUT

SUPER

0-8 Jamey Tucker/whatthetech.tv

ON-CAMERA TEASE:

IT'S A SCAM THAT SCARES PEOPLE OUT OF THOUSANDS OF DOLLARS. AND THE VICTIMS WON'T REPORT IT OR TELL ANYONE. I'M JAMEY TUCKER, COMING UP WITH A SIMPLE WAY TO FIND OUT IF AN EMAIL OR TEXT IS A SCAM.

ANCHOR INTRO

INTERNET SCAMS SEEM TO LURK AROUND EVERY CORNER, AND UNFORTUNATELY, THERE'S ONE IN PARTICULAR THAT'S BEEN QUITE SUCCESSFUL IN SEPARATING PEOPLE FROM THEIR HARD-EARNED MONEY.

THIS SCAM MAKES THE ROUNDS EVERY FEW YEARS. IT'S SCARY AND IT'S FRIGHTENING. AND CHANCES ARE YOU, OR SOMEONE YOU KNOW MIGHT HAVE FALLEN VICTIM AND WERE TOO SCARED TO TELL ANYONE.
OUR CONSUMER TECH REPORTER JAMEY TUCKER TAKES A CLOSER LOOK.

PACKAGE SCRIPT

The first time I reported on this scam was about 10 years ago. It came around again in 2020. And it's making the rounds again. One of our viewers sent me the threatening email she received just last week.

The scammer claims he purchased access to email accounts and logged into her. In detail, he says he installed software that allowed him to record her phone screen and her face. Claiming he recorded her as she looked at a porn website. And that he would release the photos everywhere unless she paid him $1,506 in Bitcoin.
It's extortion and It is a scam. Here's what you need to know:

Cybercriminals do purchase usernames and passwords on the dark web that can give them access to email accounts. This alone does not allow them to install software on devices and computers.

They can install malware on a computer by convincing you to click a link or to enter something that will give them remote access.

This is a scam. Don't fall for it. Do not pay and do NOT click on a link or open an attachment. You can often determine if something is a scam by doing a Google search.

Scammers are too lazy to rewrite these emails so they copy and paste them or send them as an image. Googling this line from the email shows the results of the exact phrase and details of the scam.

I'm glad I could help our viewer with this. And if you have questions about scams, you can reach out to me on my Facebook page. Like and follow What the Tech TV, and send me your questions. That's What the Tech? I'm Jamey Tucker

ANCHOR TAG

SEXTORTION SCAMS ARE A HUGE PROBLEM AND LARGELY GO UNREPORTED. IF YOU RECEIVE THIS SCAM YOU'RE ASKED TO FORWARD IT TO THE F.B.I.

WEB STORY

Internet scams seem to lurk around every corner, and unfortunately, there's one in particular that's been quite successful in separating people from their hard-earned money.

This scam has been making the rounds every few years, and chances are, someone you know might have fallen victim to it without ever mentioning it to anyone.

The first time this scam was brought to light was around a decade ago, and it resurfaced again in 2020. Now, cyber creeps are at it again, spreading their deceitful tactics far and wide. Just last week, one of our viewers received a threatening email and forwarded it to me. She said she was terrified and did not know what to do.

The scammer's modus operandi is to claim they've gained access to the victim's email account, alleging they've installed software to record their phone screen and face. They then threaten to release compromising photos, supposedly taken while the victim was browsing a pornographic website, unless a hefty sum of $1,506 in Bitcoin is paid.

Let's get one thing straight: this is a scam. But it's essential to understand how it operates to protect yourself:

Firstly, cybercriminals do indeed purchase usernames and passwords from the dark web, but merely having this information doesn't grant them the ability to install software on your devices.

However, they can deploy malware onto your computer by tricking you into clicking on a malicious link or providing them with remote access, often through a convincing phone call posing as technical support.

Furthermore, some victims report receiving emails containing screenshots of their faces, allegedly captured while downloading a video game or pirated software. Again, it's all part of the scam. Those victims also happened to have downloaded pirated software and video games that captured their images when they installed the program. The images and email addresses were made available for purchase on the Dark Web.

Thankfully, there are ways to discern whether an email is legitimate or a scam. A quick Google search can often reveal the truth. Scammers tend to be lazy and reuse the same email templates or send them as images. By copying and pasting a suspicious email into a search bar, you can uncover results that expose the scam for what it is.

If you ever feel threatened by an email scam, don't hesitate to take action. Remember to stay vigilant and educate yourself about the latest scams circulating on the internet.

Report this and other scams to the FBI cyber tip line: https://tips.fbi.gov/home