Sextortion:
What You Need to Know

October 31, 2023

William Favre Slater, III
M.S. in Cybersecurity
CISSP, SSCP, CISA, PMP, ITIL, IPv6
President and CISO
Slater Technologies, Inc.
Chicago, Illinois, USA

Abstract

Sextortion Attacks are on the rise. This brief Presentation will explain what Sextortion is, and what to do if you get a Sextortion e-mail or message. Sextortion is a serious crime and has caused some naïve people to pay large sums of money, or in worst cases, even commit suicide. This Presentation is presented a Public Service to help all Netizens be a little safer when using the Internet.

Disclaimer

This presentation was created as a Public Service for Cybersecurity Awareness Month – October 2023

The content in this presentation is from William Favre Slater, III, a private U. S. Citizen, & President of Slater Technologies, Inc., and his research sources. It was prepared and presented with Good Will as a Service to Benefit the Good Netizens who participate regularly in the Cyberspace created by the networks and devices that comprise Internet.

Everything presented here is true and accurate to the best of Mr. Slater's knowledge. However, it should be stated here that the targeted sexploitation attacks and accompanying accusations described in this presentation are false and completely baseless. Mr. Slater is a dedicated seasoned Cybersecurity Professional with multiple decades of experience, and does not use any of his computing devices and/or software for anything other than honorable purposes.

Mr. Slater only represents himself and is solely responsible for his comments, content, and research.

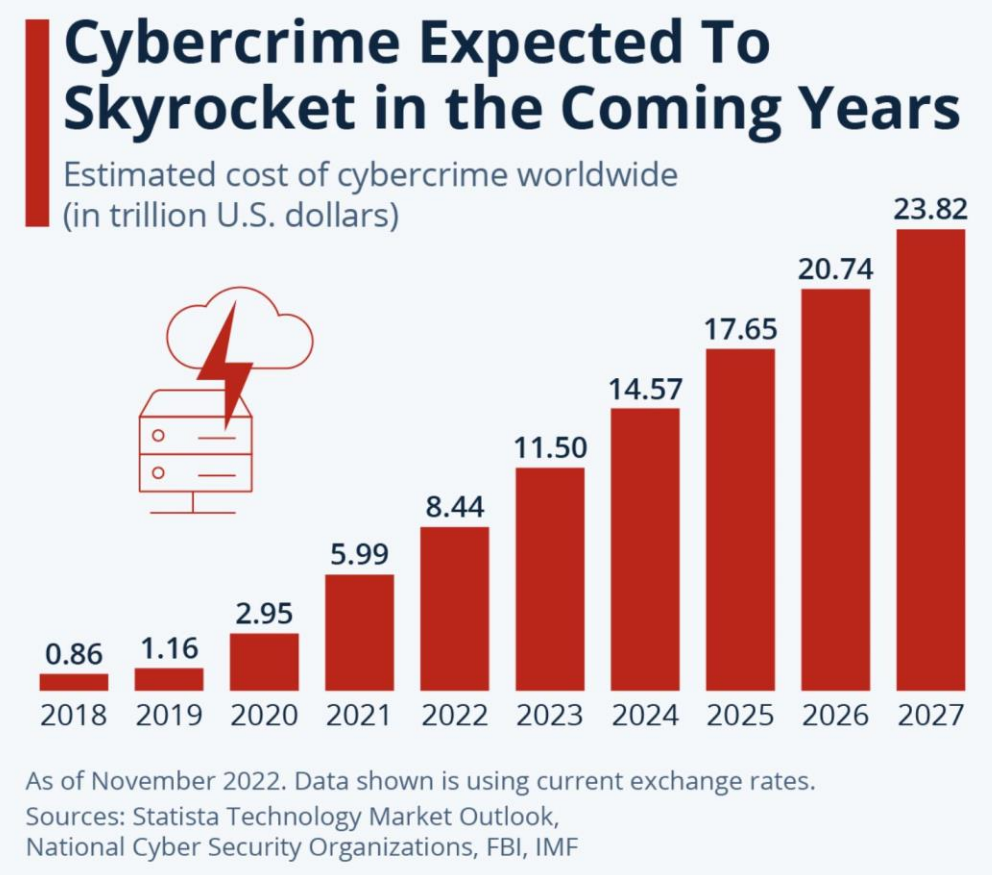
Agenda

- Introduction
- CyberCrime Is Out of Control
- What is Sextortion?
- Where, When, and How Does Sextortion Occur?
- Why Sextortion?
- Why Is Sextortion a Problem?
- What Sextortion Looks Like
- Sextortionist Attacker Campaign Timeline
- Sextortion Victim Timeline
- Finding the IP Address of Sextortion Attacker
- What's Really Happening During Your Sextortion Experience
- How Much Does the Internet Really Know About You and Your Personal Life?
- What You SHOULD Do During Your Sextortion Experience
- Exploring the Sextortionist Attacker on a Blockchain Explorer
- Finding the IP Address of Sextortionist Attacker
- Best Advice If You Are a Sextortion Target
- General Internet Safety Tips
- Conclusion

Introduction

- ***Sextortion Attacks*** are on the rise. This brief Presentation will explain what ***Sextortion*** is, what to do if you get a ***Sextortion*** e-mail or message.
- ***Sextortion*** is a serious issue and has caused some people to pay large somes of money, or in worst cases, even commit suicide.
- This Presentation is presented a Public Service to help all Netizens be a little safer when using the Internet.

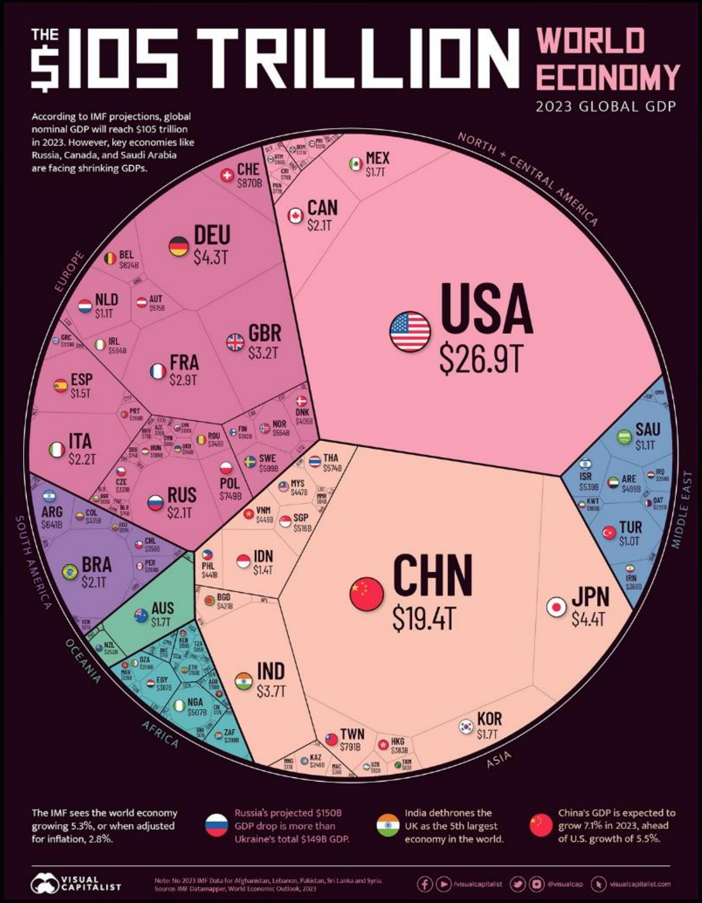
Cybercrime Is Out of Control



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF



THE $105 TRILLION WORLD ECONOMY

2023 GLOBAL GDP

According to IMF projections, global nominal GDP will reach $105 trillion in 2023. However, key economies like Russia, Canada, and Saudi Arabia are facing shrinking GDPs.

The IMF sees the world economy growing 5.3%, or when adjusted for inflation, 2.8%.

Russia's projected $150B GDP drop is more than Ukraine's total $149B GDP.

India dethrones the UK as the 5th largest economy in the world.

China's GDP is expected to grow 7.1% in 2023, ahead of U.S. growth of 5.5%.

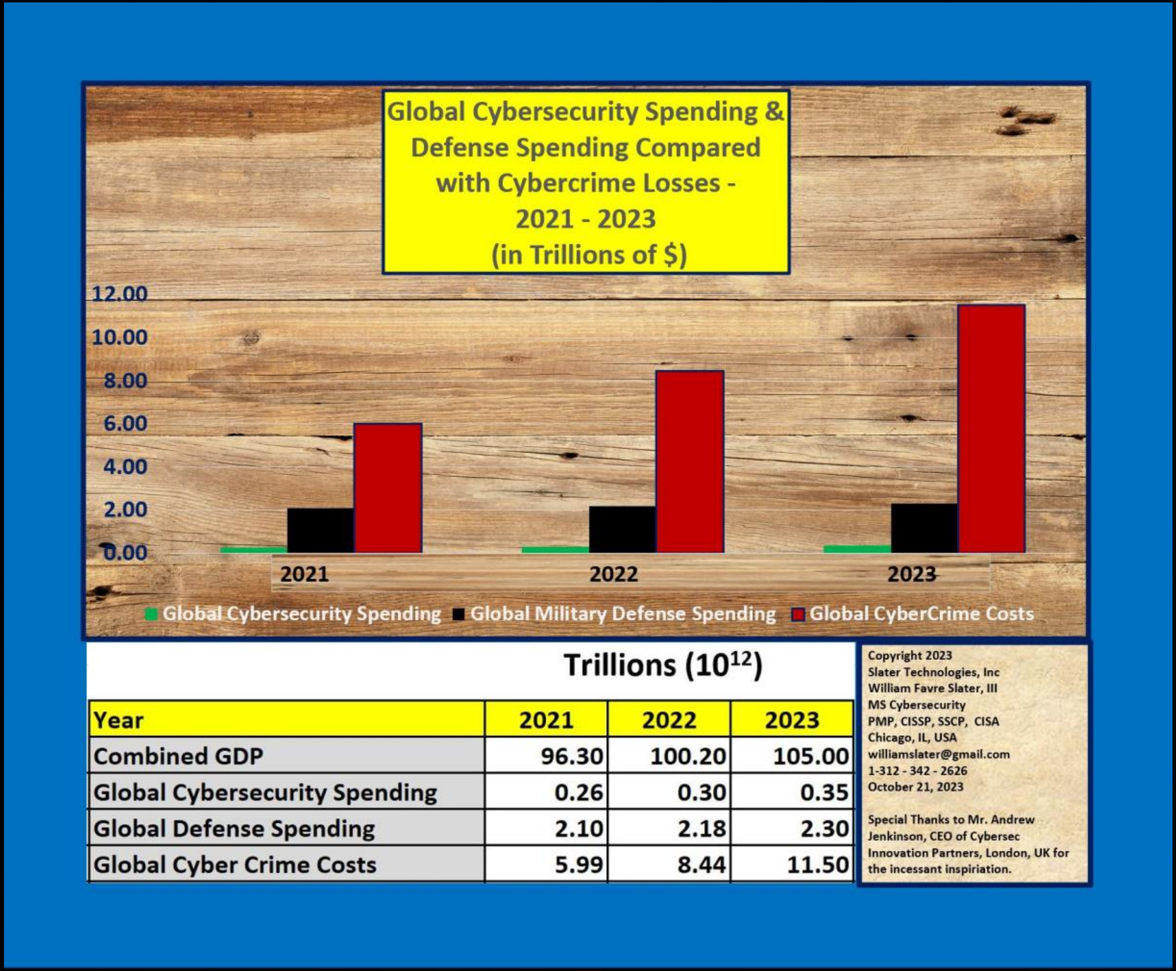
VISUAL CAPITALIST

Note: No 2023 IMF Data for Afghanistan, Lebanon, Pakistan, Sri Lanka and Syria.
Source: IMF Datamapper, World Economic Outlook, 2023

/visualcapitalist @visualcap visualcapitalist.com

If Cybercrime Crime was a Country, it would be the 3rd Richest Country in the World.

Cybercrime Is Out of Control



Trillions (10^{12})

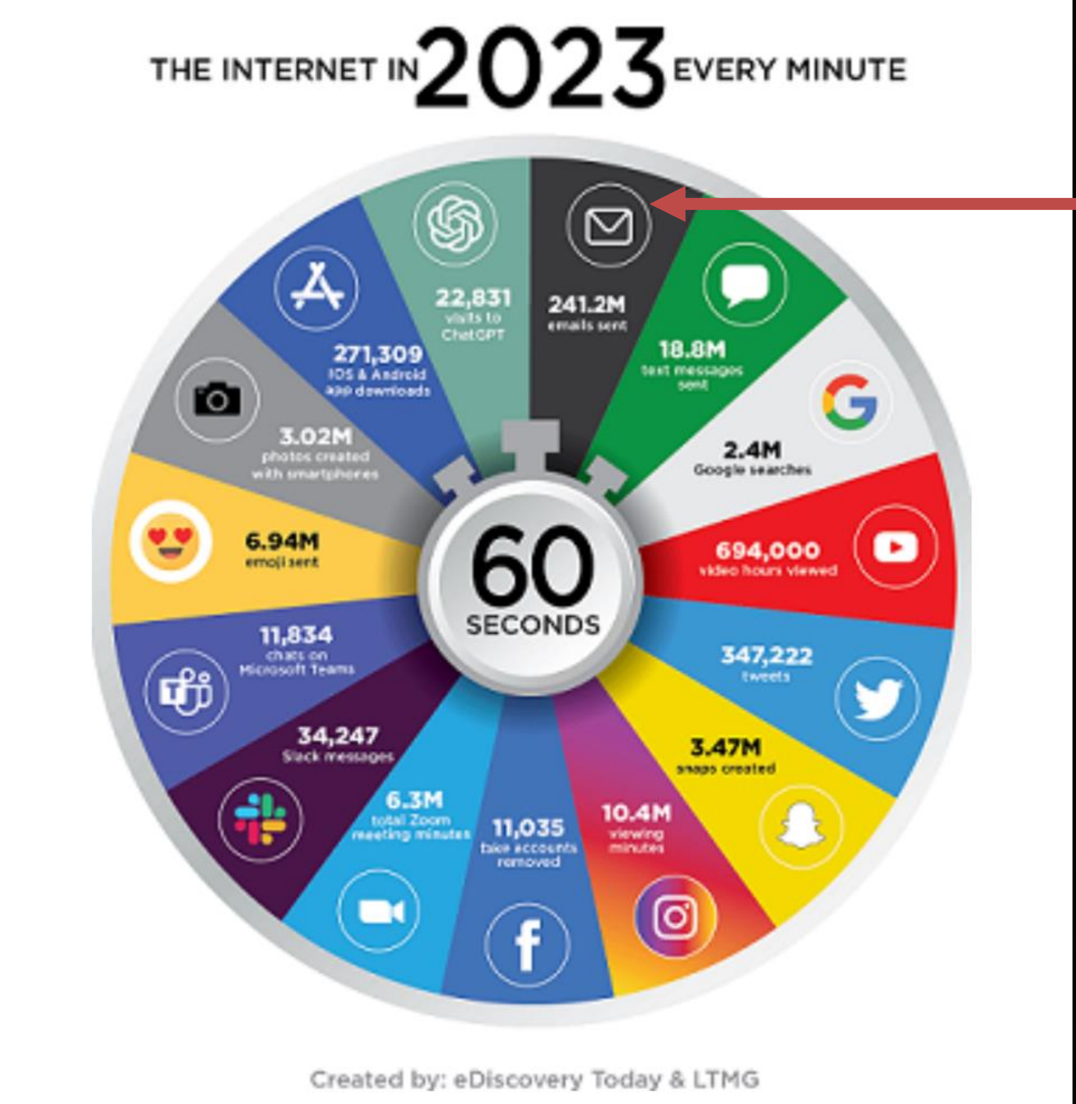
Year	2021	2022	2023
Combined GDP	96.30	100.20	105.00
Global Cybersecurity Spending	0.26	0.30	0.35
Global Defense Spending	2.10	2.18	2.30
Global Cyber Crime Costs	5.99	8.44	11.50

William Favre Slater, III
MS Cybersecurity
PMP, CISSP, SSCP, CISA
Chicago, IL, USA
williamslater@gmail.com
1-312 - 342 - 2626
October 21, 2023

Special Thanks to Mr. Andrew Jenkinson, CEO of Cybersec Innovation Partners, London, UK for the incessant inspiriation.

Cybercrime Crime Damages compared with Global Spending on Cybersecurity and Combined National Defense Budgets.

What Happens on the Internet Every 60 Seconds?



Created by: eDiscovery Today & LTMG

E-mails per minute:

241.2 Million

What Is Extortion?

- What is Extortion under California Penal Code Section 518?
- Sextortion is a type of extortion that encompasses a wide range of behaviors. Sextortion, on the other hand, differs from most other forms of extortion in that it frequently involves threats of revealing the victim’s personal, intimate images or videos if individual will not pay.

- The crime of extortion is defined as:

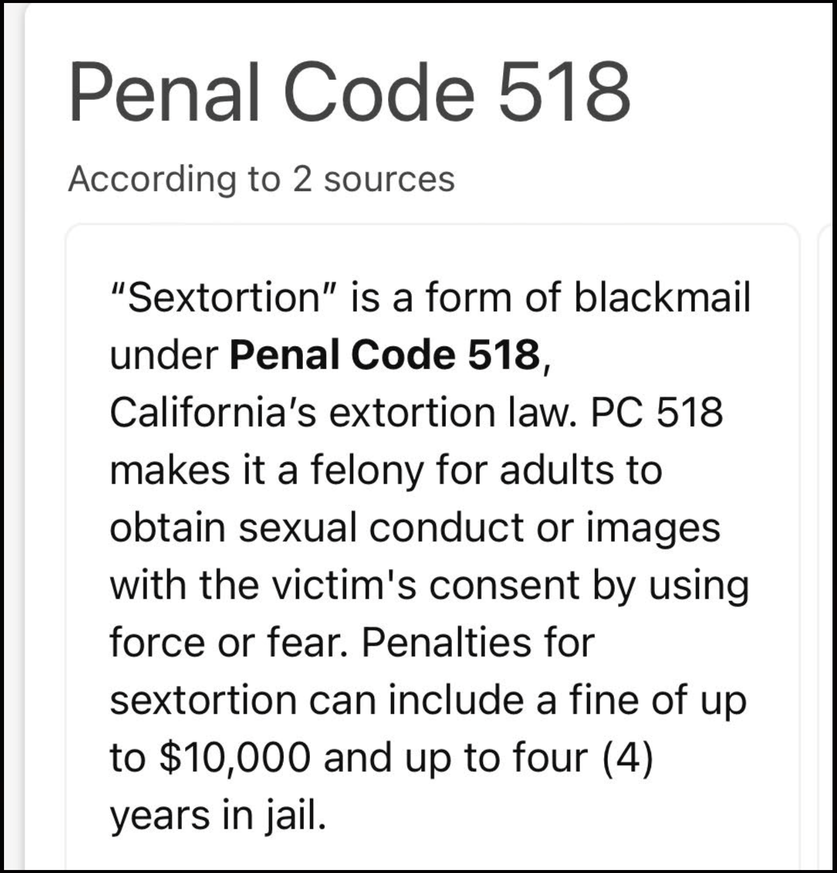
  obtaining property (other considerations)/official act of public
  with the person’s consent/under color of official right
  induced by wrongful use of fear or force

- Some sextortionists, on the other hand, use something as simple as a text message with your text messages and phone number. Victims who are in a monogamous relationship may find this information to be compromising.

Source: https://kaass.com/what-is-sextortion-under-california-law/

What Is Sextortion?

- A crime
- A form of blackmail
- A felony under California Law.



Penal Code 518

According to 2 sources

"Sextortion" is a form of blackmail under **Penal Code 518**, California's extortion law. PC 518 makes it a felony for adults to obtain sexual conduct or images with the victim's consent by using force or fear. Penalties for sextortion can include a fine of up to $10,000 and up to four (4) years in jail.

Source: https://wikipedia.org/

What Is Sextortion?

- Sextortion is a serious crime in which a perpetrator threatens to publish private and explicit information or material about you (or to share it with your friends and family) unless you comply with their demands. The demand for sexual images, money, or sexual favors is common.

- The goal of a sextortionist is to make you fear that he will share your private photos or videos online for all of your friends, family, and coworkers to see. Criminals use your fear to force you to pay them in exchange for not releasing your personal photos, videos, or other media.

- Starting from 2018 California Penal Code amended the law on the criminalization of extortion and added points with regards to “sextortion” crime.

Source: https://kaass.com/what-is-sextortion-under-california-law/

What Is Sextortion?

- What is Sextortion under California Law?
  - Under California’s extortion law, Penal Code 518, “sextortion” is a type of blackmail. The term “extortion” is defined in California law.
  - Sextortion is defined by obtaining:
    - an image of an intimate body part of the victim
    - demanding sexual conduct
    - by wrongful use of fear or force
  - In other words, sextortion is a form of extortion in cases in which the perpetrator threatens the victim to release information (mostly concerning intimate information on the victim) demanding money, or sexual favors, personal media.

Source: https://kaass.com/what-is-sextortion-under-california-law/

Where, When, and How Does Sextortion Occur?

- Where: Across the Internet to your Desktop Computer, Laptop, or SmartPhone

- When: Anytime of day

- How: Your e-mail address or phone number is acquired by the Sextortion Attacker from people who harvest e-mails and sell them. The Sextortion Attacker uses the e-mail or your phone number to conduct his attack.

Why Is Sextortion a Problem?

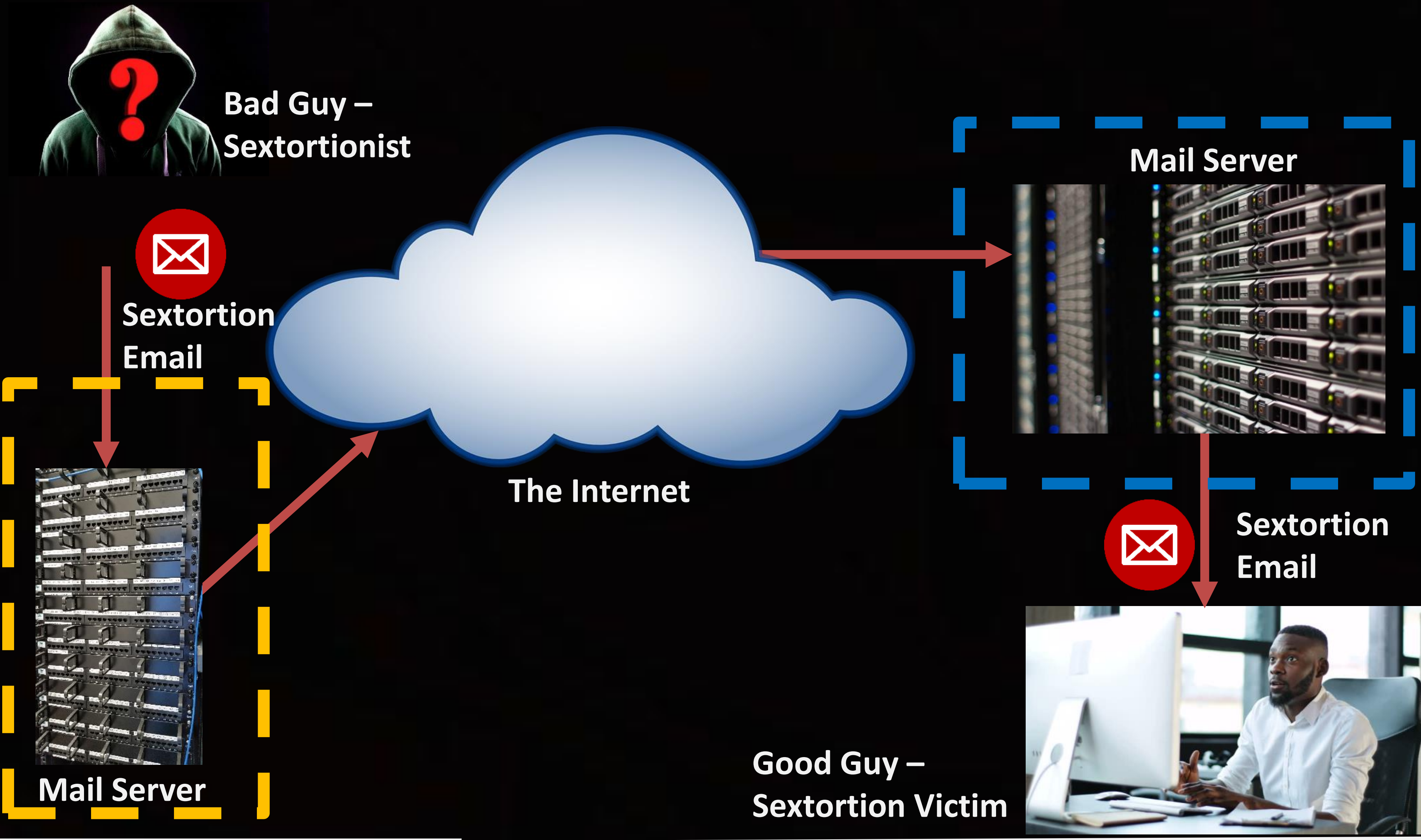
- Sextortion is a problem because it attempts to use fear to induce an Internet user to pay a large amount of money in Cryptocurrency (Digital Money).

- Some Sextortion victims do drastic things like committing suicide

- Sextortion is a Felony in California, since 2018.

- We are now all connected to the Internet at various times in multiple ways. The Internet has unfortunately become a gigantic “Electronic Cesspool”.

What Sextortion Looks Like



Bad Guy – Sextortionist

Sextortion Email

Mail Server

The Internet

Mail Server

Sextortion Email

Good Guy – Sextortion Victim

What Sextortion Looks Like (1 of 3)

Hello there!

Unfortunately, there are some bad news for you.

Some time ago your device was infected with my private trojan, R.A.T (Remote Administration T
if you want to find out more about it simply use Google.

My trojan allowed me to access your files, accounts and your camera.

Check the sender of this email, I have sent it from your email account.

You truly enjoy checking out porn websites and watching dirty videos, while having a lot of kink

I RECORDED YOU (through your camera) SATISFYING YOURSELF!

After that I removed my malware to not leave any traces.

What Sextortion Looks Like (2 of 3)

If you still doubt my serious intentions, it only takes couple mouse clicks to share the video of you with your friends, relatives, all email contacts, on social networks, the darknet and to publish all your files.

All you need is $1400 USD in Bitcoin (BTC) transfer to my account (Bitcoin equivalent based on exchange rate during your transfer).

After the transaction is successful, I will proceed to delete everything without delay.

Be sure, I keep my promises.

You can easily buy Bitcoin (BTC) here: www.paxful.com , www.coingate.com , www.coinbase.com , or check for Bitcoin (BTC) ATM near you, or Google for other exchanger.

You can send the Bitcoin (BTC) directly to my wallet, or install the free software: Atomicwallet, or: Exodus wallet, then receive and send to mine.

What Sextortion Looks Like (3 of 3)

My Bitcoin (BTC) address is: 1CK41adce6KuM3UM2eySnzUyR9SAJnf4wu

Yes, that's how the address looks like, copy and paste my address, it's (cAsE-sEnSEtiVE).

You are given not more than 2 days after you have opened this email.

As I got access to this email account, I will know if this email has already been read.

Everything will be carried out based on fairness.

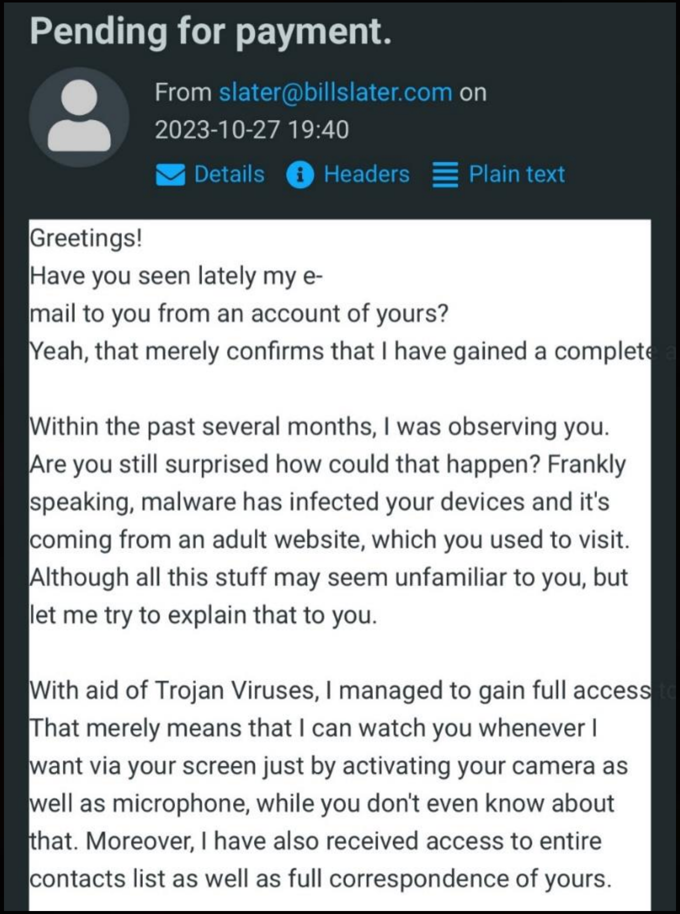
An advice from me, regularly change all your passwords to your accounts and update your device with newest security patches.

As I got access to this email account, I will know if this email has already been read.

Everything will be carried out based on fairness.

An advice from me, regularly change all your passwords to your accounts and update your devic with newest security patches.

What Sextortion Looks Like - 2nd Example (1 of 2)



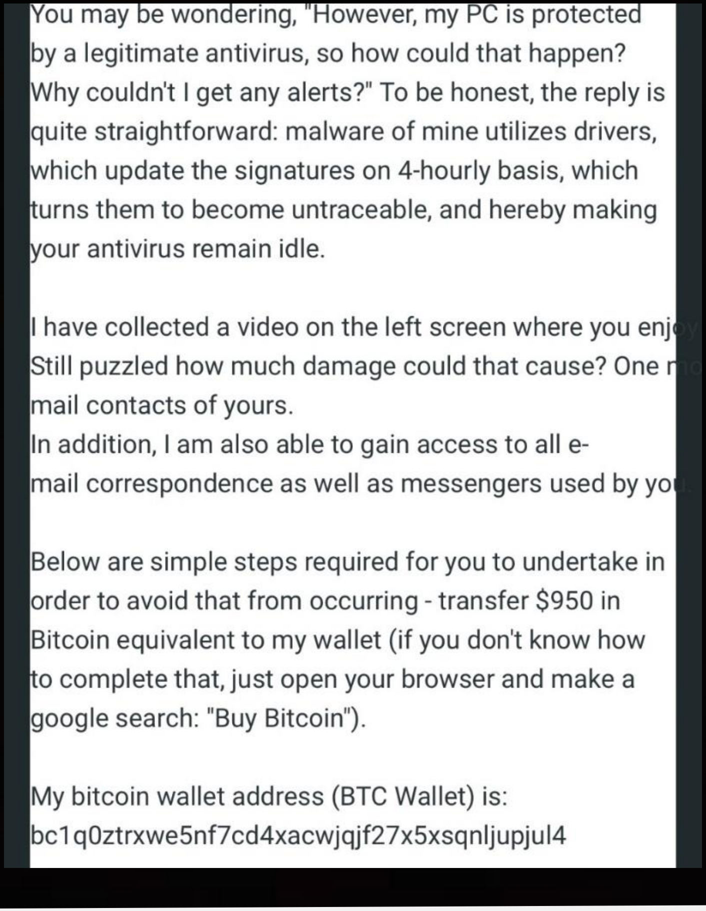
Pending for payment.

From slater@billslater.com on
2023-10-27 19:40

Greetings!
Have you seen lately my e-mail to you from an account of yours?
Yeah, that merely confirms that I have gained a complete a

Within the past several months, I was observing you.
Are you still surprised how could that happen? Frankly speaking, malware has infected your devices and it's coming from an adult website, which you used to visit.
Although all this stuff may seem unfamiliar to you, but let me try to explain that to you.

With aid of Trojan Viruses, I managed to gain full access to
That merely means that I can watch you whenever I want via your screen just by activating your camera as well as microphone, while you don't even know about that. Moreover, I have also received access to entire contacts list as well as full correspondence of yours.



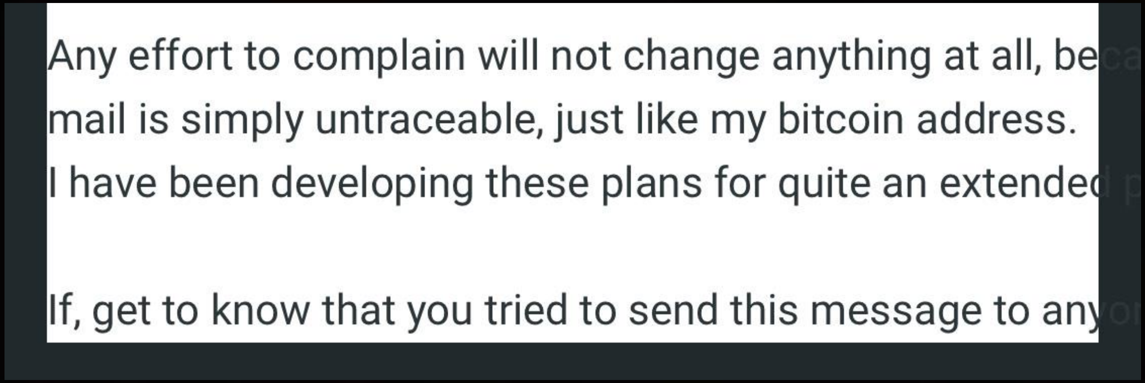
You may be wondering, "However, my PC is protected by a legitimate antivirus, so how could that happen? Why couldn't I get any alerts?" To be honest, the reply is quite straightforward: malware of mine utilizes drivers, which update the signatures on 4-hourly basis, which turns them to become untraceable, and hereby making your antivirus remain idle.

I have collected a video on the left screen where you enjoy
Still puzzled how much damage could that cause? One mo
mail contacts of yours.
In addition, I am also able to gain access to all e-mail correspondence as well as messengers used by you.

Below are simple steps required for you to undertake in order to avoid that from occurring - transfer $950 in Bitcoin equivalent to my wallet (if you don't know how to complete that, just open your browser and make a google search: "Buy Bitcoin").

My bitcoin wallet address (BTC Wallet) is:
bc1q0ztrxwe5nf7cd4xacwjqjf27x5xsqnljupjul4

What Sextortion Looks Like - 2nd Example (2 of 2)



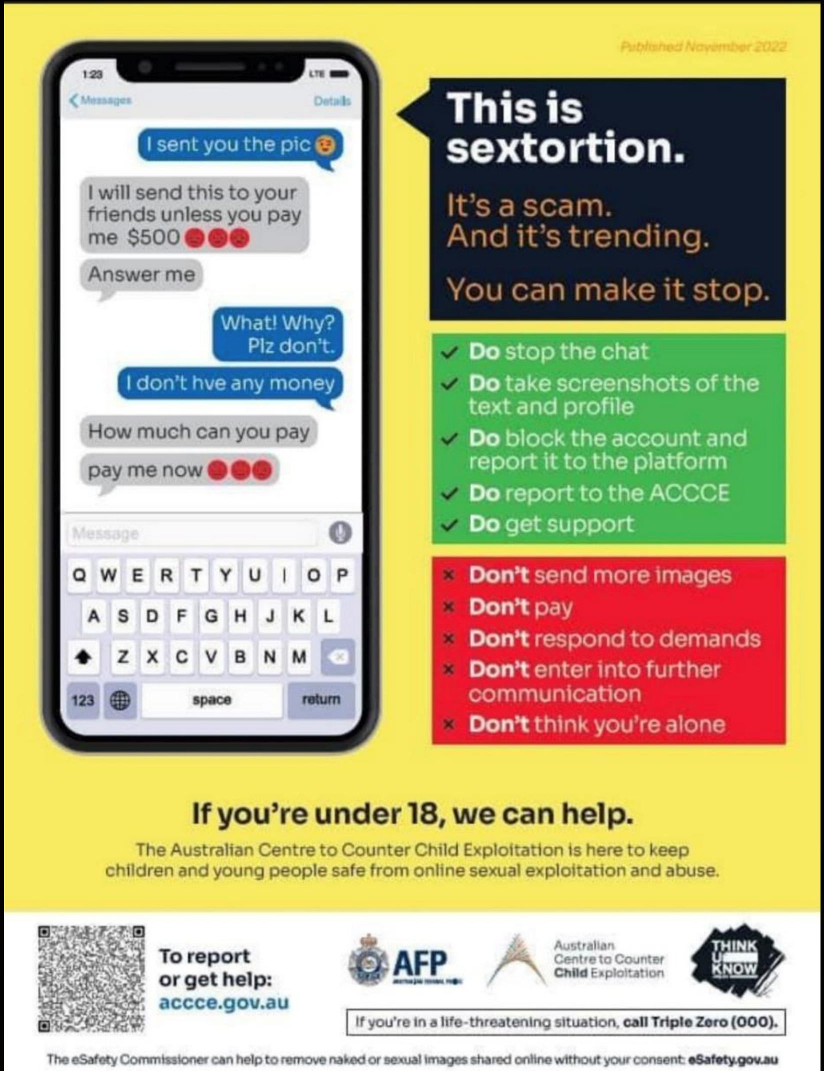
Any effort to complain will not change anything at all, beca

mail is simply untraceable, just like my bitcoin address.

I have been developing these plans for quite an extended p

If, get to know that you tried to send this message to anyo

What Sextortion Also Looks Like


1:23
Messages
Details
Message
space
return

Published November 2022

I sent you the pic

I will send this to your friends unless you pay me $500

Answer me

What! Why? Plz don't.

I don't hve any money

How much can you pay

pay me now

This is sextortion.

It's a scam. And it's trending.

You can make it stop.

- ✓ **Do** stop the chat
- ✓ **Do** take screenshots of the text and profile
- ✓ **Do** block the account and report it to the platform
- ✓ **Do** report to the ACCCE
- ✓ **Do** get support

- × **Don't** send more images
- × **Don't** pay
- × **Don't** respond to demands
- × **Don't** enter into further communication
- × **Don't** think you're alone

If you're under 18, we can help.

The Australian Centre to Counter Child Exploitation is here to keep children and young people safe from online sexual exploitation and abuse.

To report or get help: accce.gov.au

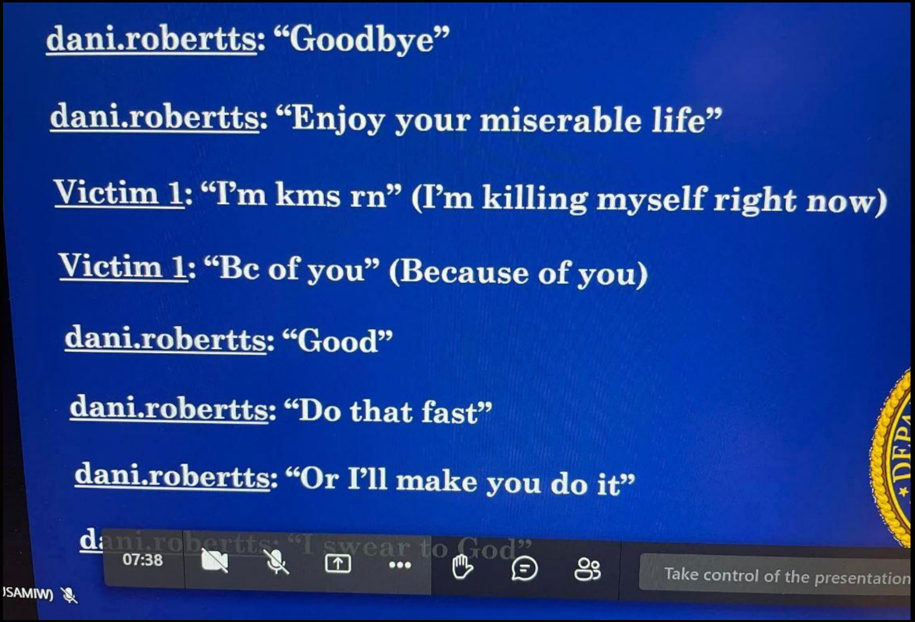
AFP

Australian Centre to Counter **Child** Exploitation

THINK U KNOW

If you're in a life-threatening situation, **call Triple Zero (000).**

The eSafety Commissioner can help to remove naked or sexual images shared online without your consent: **eSafety.gov.au**



dani.robertts: "Goodbye"

dani.robertts: "Enjoy your miserable life"

Victim 1: "I'm kms rn" (I'm killing myself right now)

Victim 1: "Bc of you" (Because of you)

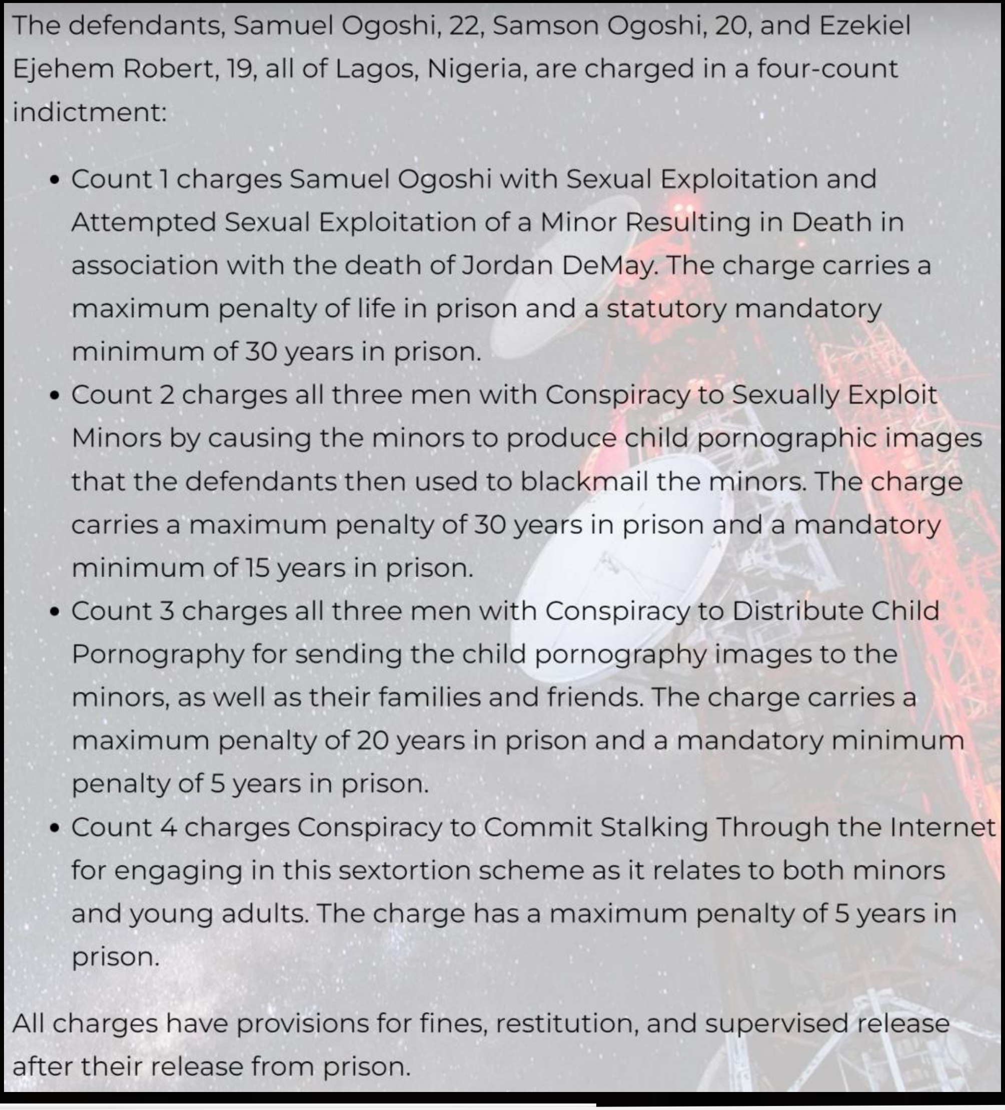
dani.robertts: "Good"

dani.robertts: "Do that fast"

dani.robertts: "Or I'll make you do it"

dani.robertts: "I swear to God"

Accused Sextortionists



The defendants, Samuel Ogoshi, 22, Samson Ogoshi, 20, and Ezekiel Ejehem Robert, 19, all of Lagos, Nigeria, are charged in a four-count indictment:

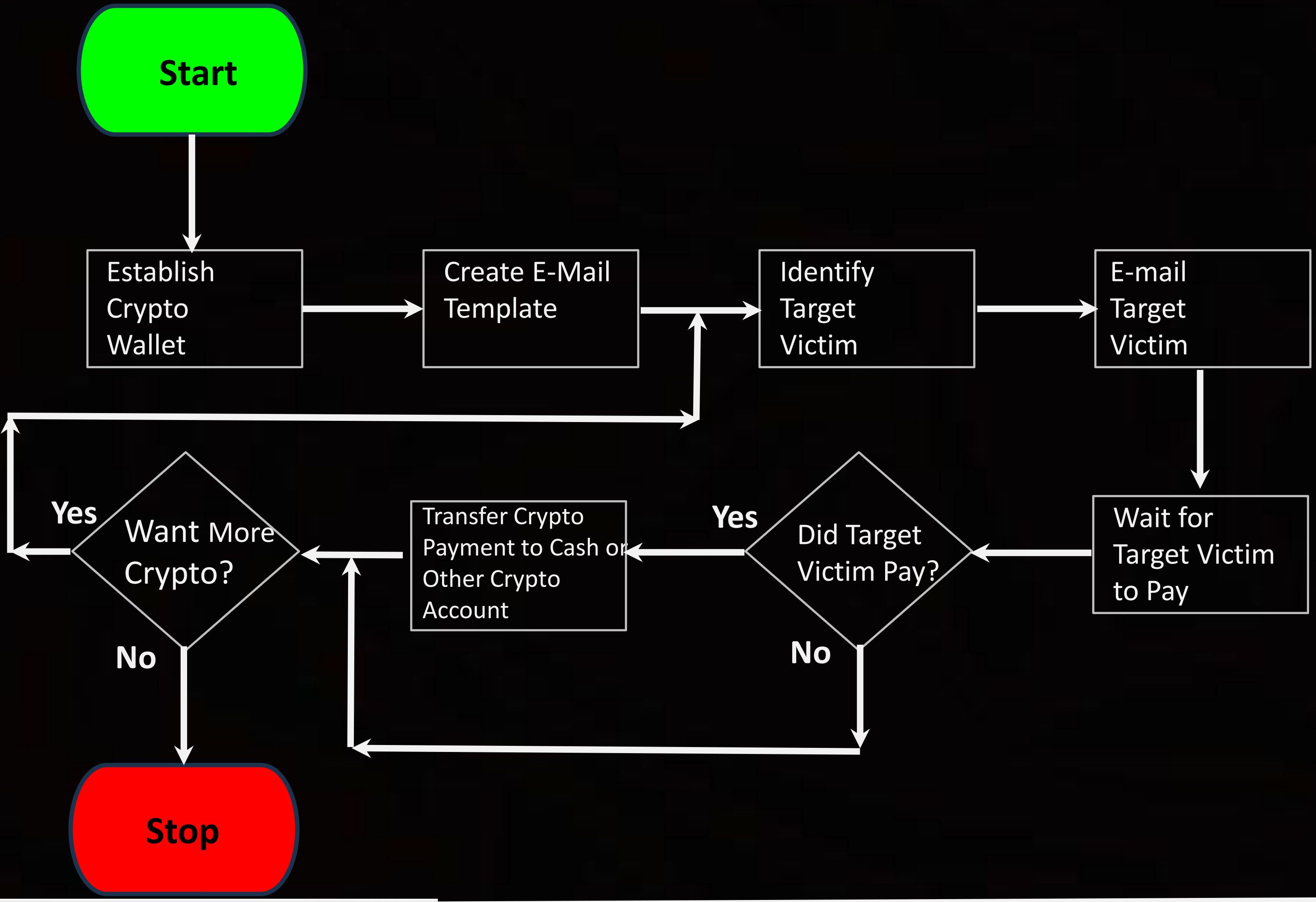
- Count 1 charges Samuel Ogoshi with Sexual Exploitation and Attempted Sexual Exploitation of a Minor Resulting in Death in association with the death of Jordan DeMay. The charge carries a maximum penalty of life in prison and a statutory mandatory minimum of 30 years in prison.
- Count 2 charges all three men with Conspiracy to Sexually Exploit Minors by causing the minors to produce child pornographic images that the defendants then used to blackmail the minors. The charge carries a maximum penalty of 30 years in prison and a mandatory minimum of 15 years in prison.
- Count 3 charges all three men with Conspiracy to Distribute Child Pornography for sending the child pornography images to the minors, as well as their families and friends. The charge carries a maximum penalty of 20 years in prison and a mandatory minimum penalty of 5 years in prison.
- Count 4 charges Conspiracy to Commit Stalking Through the Internet for engaging in this sextortion scheme as it relates to both minors and young adults. The charge has a maximum penalty of 5 years in prison.

All charges have provisions for fines, restitution, and supervised release after their release from prison.

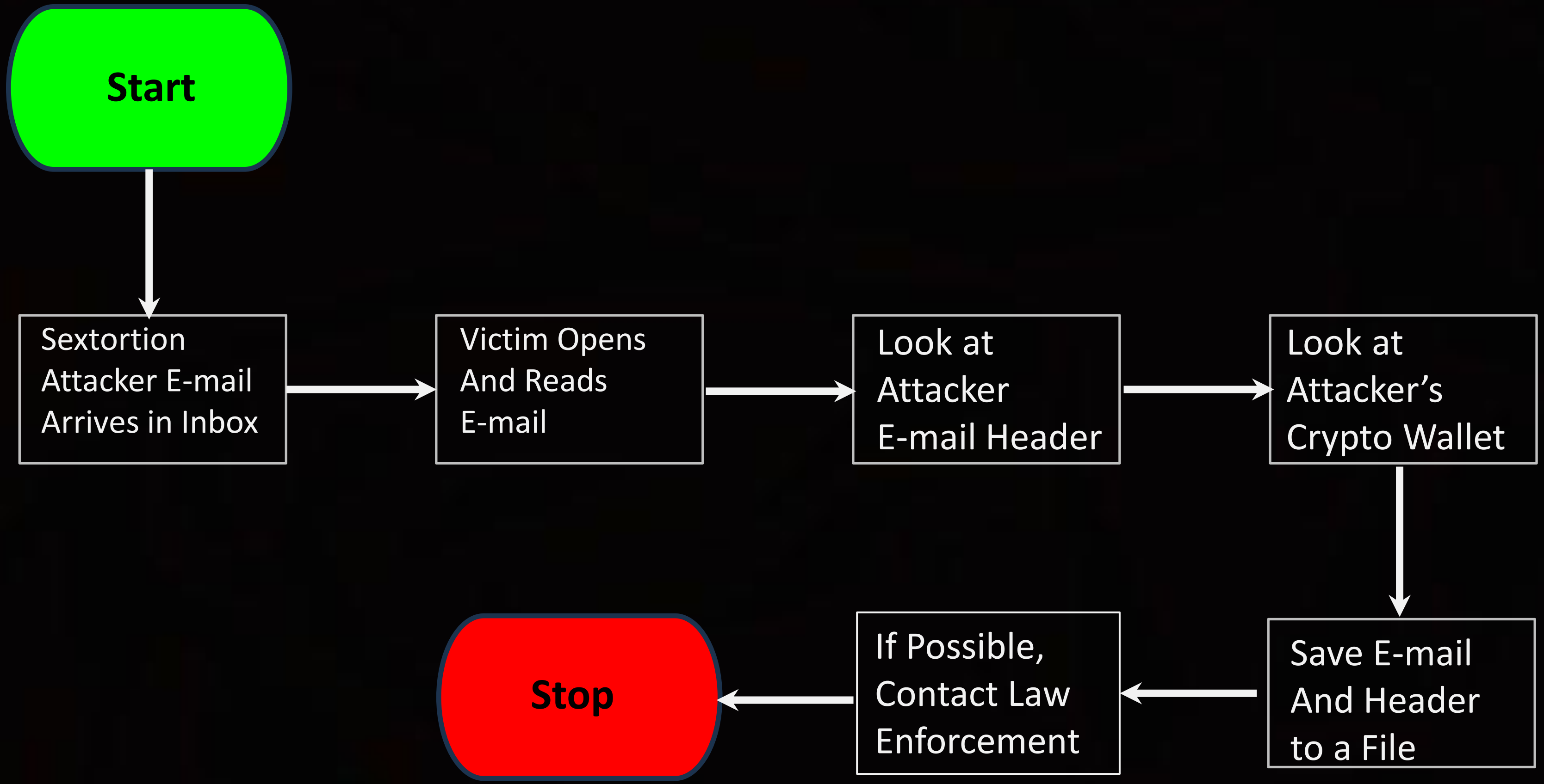
Samuel Ogoshi, 22, Samson Ogoshi, 20, and Ezekiel Ejehem Robert, 19, all of Lagos, Nigeria

Source: Hall, J. (2023) "Three Nigerians Charged In Sextortion Connected To Marquette Teen's Suicide". Published at Radio Results Network. May 3, 2023. Retrieved from https://www.radioresultsnetwork.com/2023/05/03/breaking-three-nigerians-charged-in-sextorton-connected-to-marquette-teens-suicide/ .

Sextortionist Attacker Campaign Timeline



Sextortion Victim Timeline


Start
Sextortion Attacker E-mail Arrives in Inbox
Victim Opens And Reads E-mail
Look at Attacker E-mail Header
Look at Attacker’s Crypto Wallet
Save E-mail And Header to a File
If Possible, Contact Law Enforcement
Stop

What's Really Happening During Your Sextortion Experience?

- The Sextortionist is attempting frighten the Sextortion Victim badly enough so they will pay the requested amount in full.
- However, 99% of the time, it is bluffing. The Sextortionist will do nothing if you ignore them, because most of us have significant digital footprints on the Internet.
- Sextortion can also be thought of as Doxxing for Money.   Doxxing is where the attacker collects every piece of digital information and posts it on the Internet in order to destroy a person's life and reputation.

How Much Does the Internet Really Know About You and Your Personal Life?

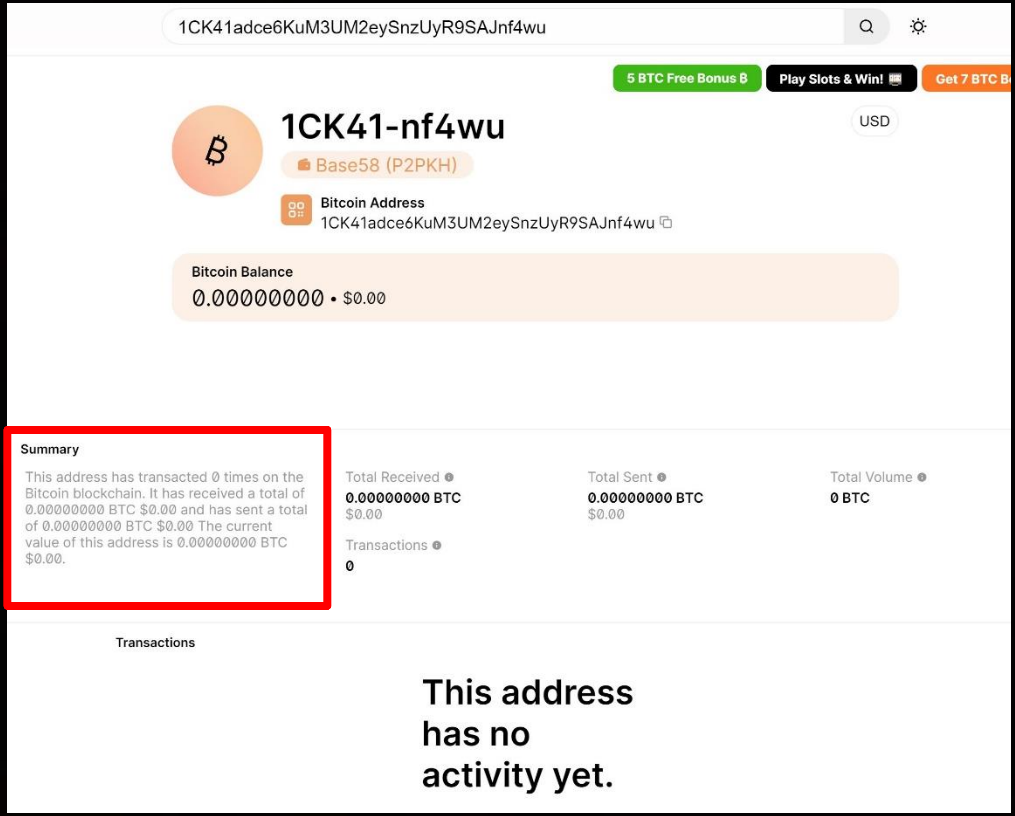
- Visit either or both of these two links to find out:
  - 1) (FREE) https://billslater.com/writing/beanonymous.pdf
  - 2) (Paid Service) https://truthfinder.com

What You SHOULD Do During Your Sextortion Experience?

- Keep calm.
- Save the e-mail.
- Save the E-Mail Header to a file.
- Copy and save the Sextortion Attacker’s message and Cryptocurrency Wallet Address.
- Look up the Sextortion Attacker’s Wallet on the Blockchain Explorer and take a screenshot.
- Look up the Sextortion Attacker’s E-mail Server IP Address, copy and save it to a file.
- Contact Law Enforcement Authorities if possible. But caution, it’s very difficult to catch and prosecute a Sextortionist.

Exploring the Sextortionist Attacker on a Blockchain Explorer – Example 1

-0- Transactions



1CK41adce6KuM3UM2eySnzUyR9SAJnf4wu

1CK41-nf4wu

Base58 (P2PKH)

Bitcoin Address
1CK41adce6KuM3UM2eySnzUyR9SAJnf4wu

Bitcoin Balance
0.00000000 • $0.00

Summary

This address has transacted 0 times on the Bitcoin blockchain. It has received a total of 0.00000000 BTC $0.00 and has sent a total of 0.00000000 BTC $0.00 The current value of this address is 0.00000000 BTC $0.00.

Total Received
0.00000000 BTC
$0.00

Total Sent
0.00000000 BTC
$0.00

Total Volume
0 BTC

Transactions
0

Transactions

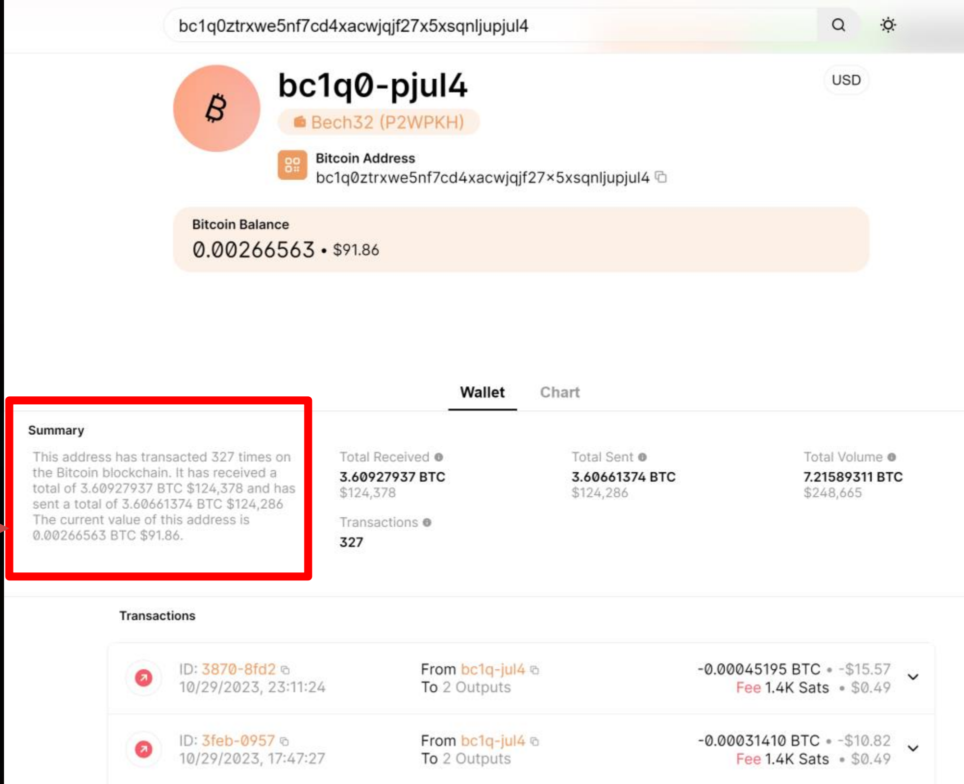
This address has no activity yet.

Website URL: https://www.blockchain.com/explorer

Crypto Wallet Address: 1CK41adce6KuM3UM2eySnzUyR9SAJnf4wu

Exploring the Sextortionist Attacker on a Blockchain Explorer – Example 2

327 Transactions



bc1q0ztrxwe5nf7cd4xacwjqjf27x5xsqnljupjul4

bc1q0-pjul4

Bech32 (P2WPKH)

USD

Bitcoin Address
bc1q0ztrxwe5nf7cd4xacwjqjf27×5xsqnljupjul4

Bitcoin Balance
0.00266563 • $91.86

Wallet Chart

Summary

This address has transacted 327 times on the Bitcoin blockchain. It has received a total of 3.60927937 BTC $124,378 and has sent a total of 3.60661374 BTC $124,286 The current value of this address is 0.00266563 BTC $91.86.

Total Received
3.60927937 BTC
$124,378

Total Sent
3.60661374 BTC
$124,286

Total Volume
7.21589311 BTC
$248,665

Transactions
327

Transactions

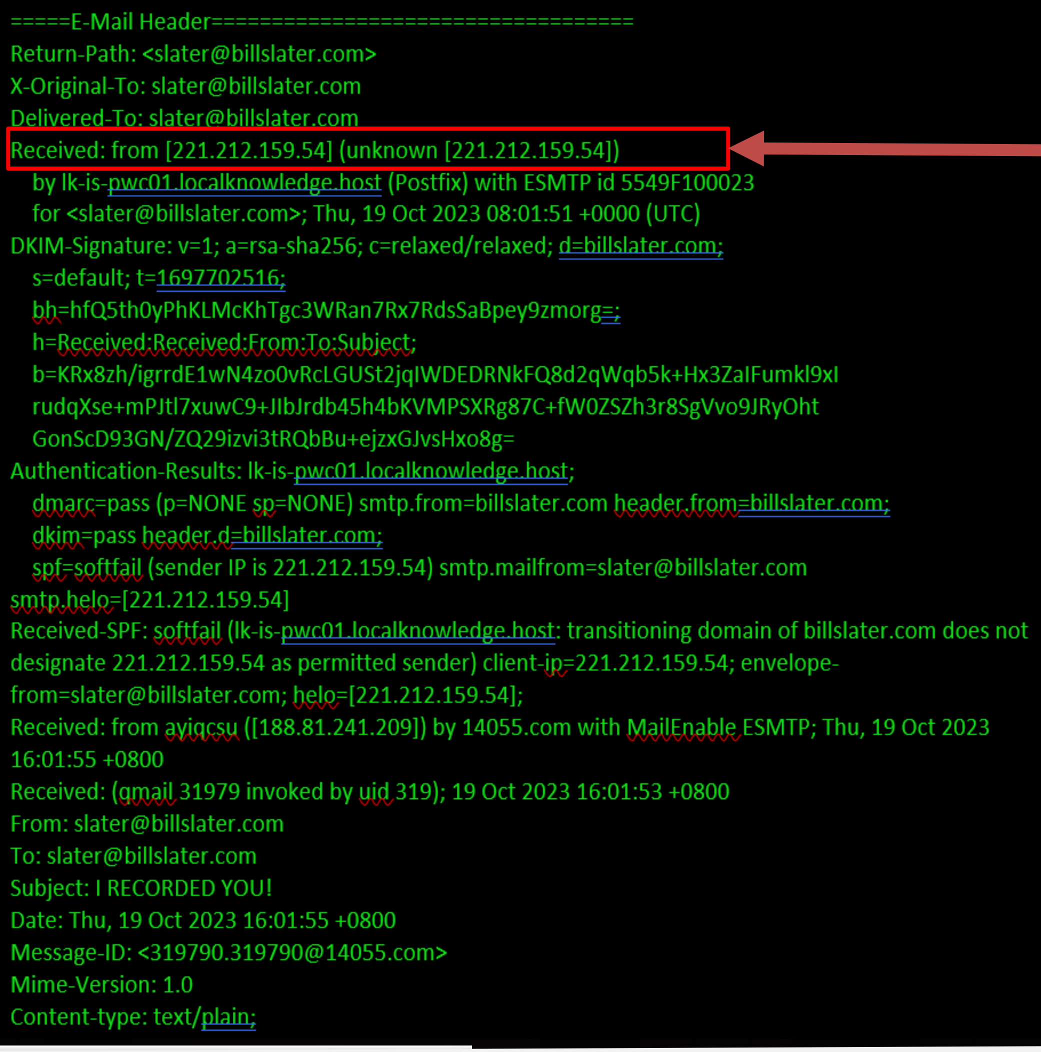
ID: 3870-8fd2
10/29/2023, 23:11:24
From bc1q-jul4
To 2 Outputs
-0.00045195 BTC • -$15.57
Fee 1.4K Sats • $0.49

ID: 3feb-0957
10/29/2023, 17:47:27
From bc1q-jul4
To 2 Outputs
-0.00031410 BTC • -$10.82
Fee 1.4K Sats • $0.49

Website URL: https://www.blockchain.com/explorer

Crypto Wallet Address: bc1q0ztrxwe5nf7cd4xacwjqjf27x5xsqnljupjul4

Finding the IP Address of Sextortionist Attacker's E-mail Server – Example 1

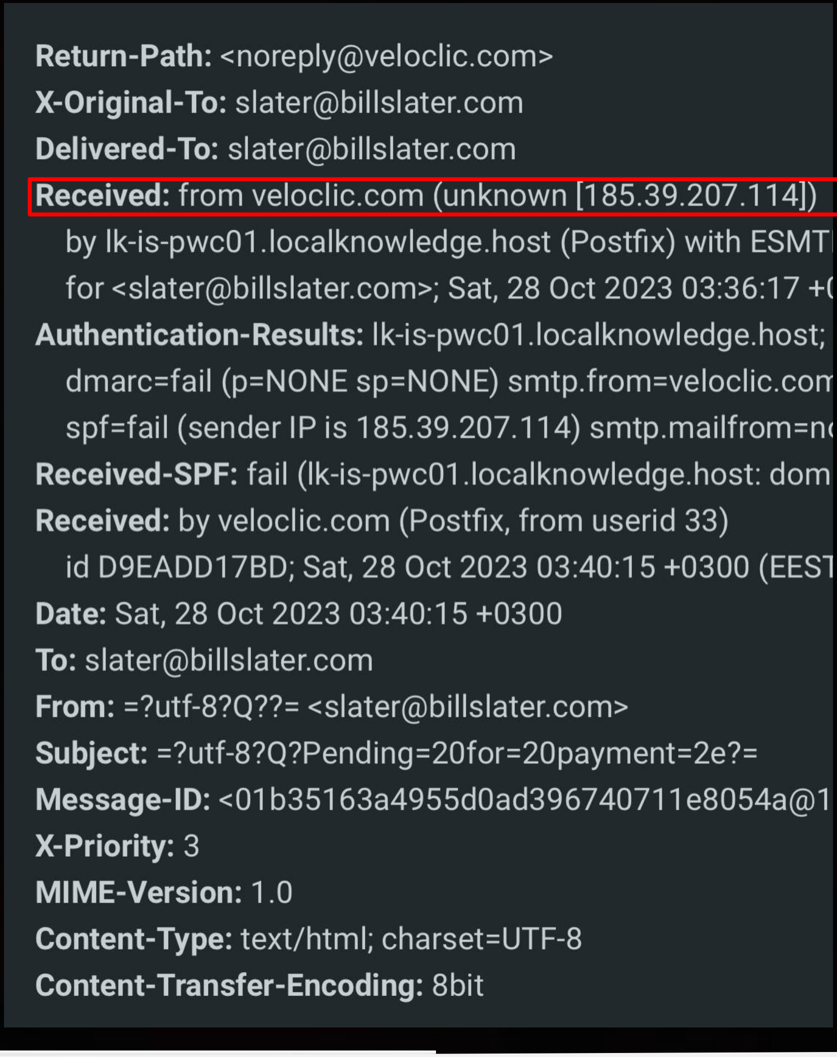


```
=====E-Mail Header==================================
Return-Path: <slater@billslater.com>
X-Original-To: slater@billslater.com
Delivered-To: slater@billslater.com
Received: from [221.212.159.54] (unknown [221.212.159.54])
   by lk-is-pwc01.localknowledge.host (Postfix) with ESMTP id 5549F100023
   for <slater@billslater.com>; Thu, 19 Oct 2023 08:01:51 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=billslater.com;
   s=default; t=1697702516;
   bh=hfQ5th0yPhKLMcKhTgc3WRan7Rx7RdsSaBpey9zmorg=;
   h=Received:Received:From:To:Subject;
   b=KRx8zh/igrrdE1wN4zo0vRcLGUSt2jqIWDEDRNkFQ8d2qWqb5k+Hx3ZaIFumkl9xl
   rudqXse+mPJtl7xuwC9+JIbJrdb45h4bKVMPSXRg87C+fW0ZSZh3r8SgVvo9JRyOht
   GonScD93GN/ZQ29izvi3tRQbBu+ejzxGJvsHxo8g=
Authentication-Results: lk-is-pwc01.localknowledge.host;
   dmarc=pass (p=NONE sp=NONE) smtp.from=billslater.com header.from=billslater.com;
   dkim=pass header.d=billslater.com;
   spf=softfail (sender IP is 221.212.159.54) smtp.mailfrom=slater@billslater.com
smtp.helo=[221.212.159.54]
Received-SPF: softfail (lk-is-pwc01.localknowledge.host: transitioning domain of billslater.com does not
designate 221.212.159.54 as permitted sender) client-ip=221.212.159.54; envelope-
from=slater@billslater.com; helo=[221.212.159.54];
Received: from ayiqcsu ([188.81.241.209]) by 14055.com with MailEnable ESMTP; Thu, 19 Oct 2023
16:01:55 +0800
Received: (qmail 31979 invoked by uid 319); 19 Oct 2023 16:01:53 +0800
From: slater@billslater.com
To: slater@billslater.com
Subject: I RECORDED YOU!
Date: Thu, 19 Oct 2023 16:01:55 +0800
Message-ID: <319790.319790@14055.com>
Mime-Version: 1.0
Content-type: text/plain;
```

Sextortion Attacker Mail Server IP Address:

221.212.159.54

Finding the IP Address of Sextortionist Attacker’s E-mail Server – Example 2



```
Return-Path: <noreply@veloclic.com>
X-Original-To: slater@billslater.com
Delivered-To: slater@billslater.com
Received: from veloclic.com (unknown [185.39.207.114])
   by lk-is-pwc01.localknowledge.host (Postfix) with ESMT
   for <slater@billslater.com>; Sat, 28 Oct 2023 03:36:17 +(
Authentication-Results: lk-is-pwc01.localknowledge.host;
   dmarc=fail (p=NONE sp=NONE) smtp.from=veloclic.con
   spf=fail (sender IP is 185.39.207.114) smtp.mailfrom=n
Received-SPF: fail (lk-is-pwc01.localknowledge.host: dom
Received: by veloclic.com (Postfix, from userid 33)
   id D9EADD17BD; Sat, 28 Oct 2023 03:40:15 +0300 (EEST
Date: Sat, 28 Oct 2023 03:40:15 +0300
To: slater@billslater.com
From: =?utf-8?Q??= <slater@billslater.com>
Subject: =?utf-8?Q?Pending=20for=20payment=2e?=
Message-ID: <01b35163a4955d0ad396740711e8054a@1
X-Priority: 3
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 8bit
```

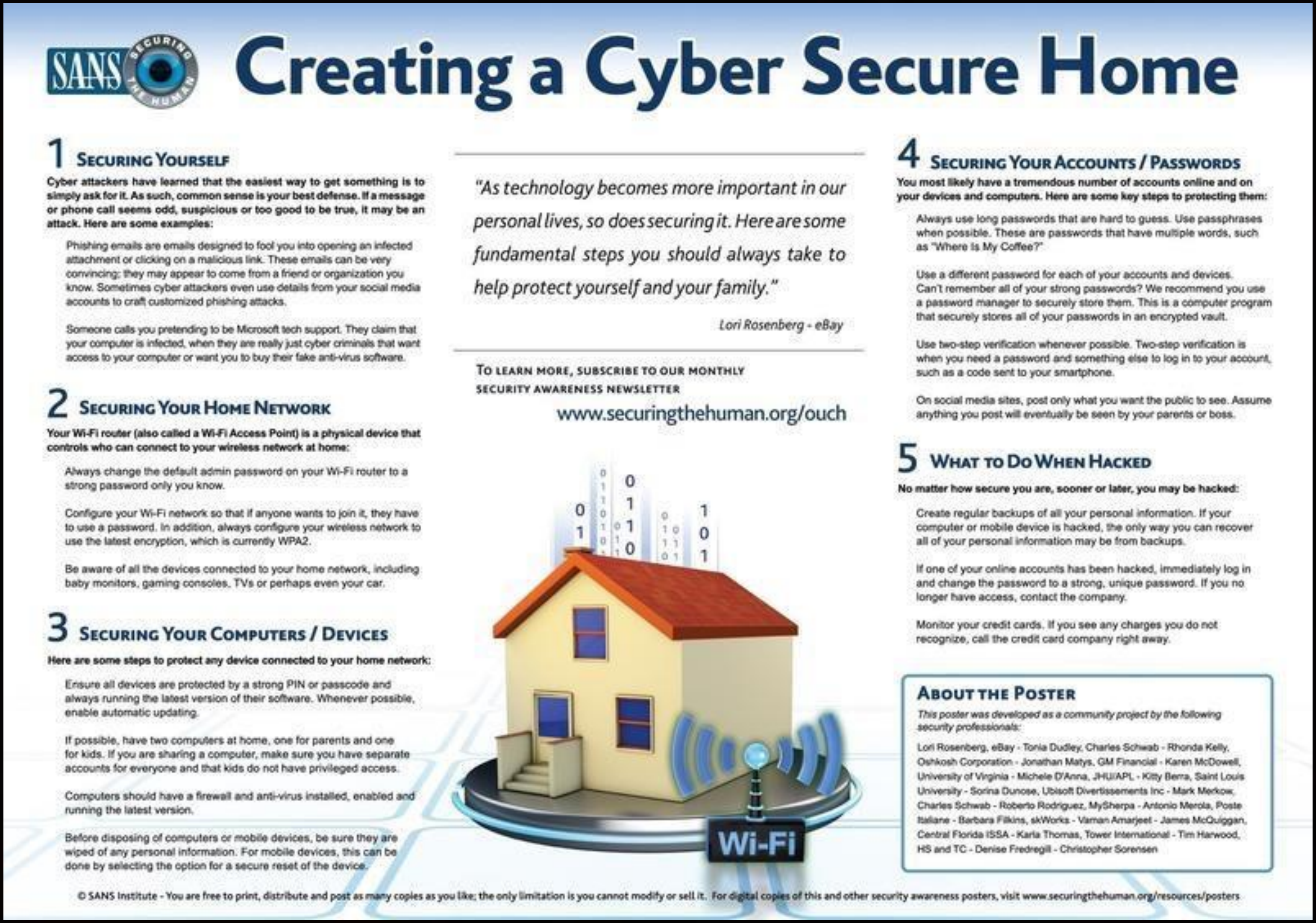
Sextortion Attacker Mail Server IP Address:

185.39.207.114

Best Advice If You Are a Sextortion Target

- Don’t panic.
- Ignore the communication.
- If possible, save the information (e-mail and e-mail header).
- Report the Sextortionist to Law Enforcement Authorities.

General Internet User Safety Tips


SANS
SECURING THE HUMAN
Wi-Fi

Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

> *"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."*
>
> *Lori Rosenberg - eBay*

To learn more, subscribe to our monthly security awareness newsletter
www.securingthehuman.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where Is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

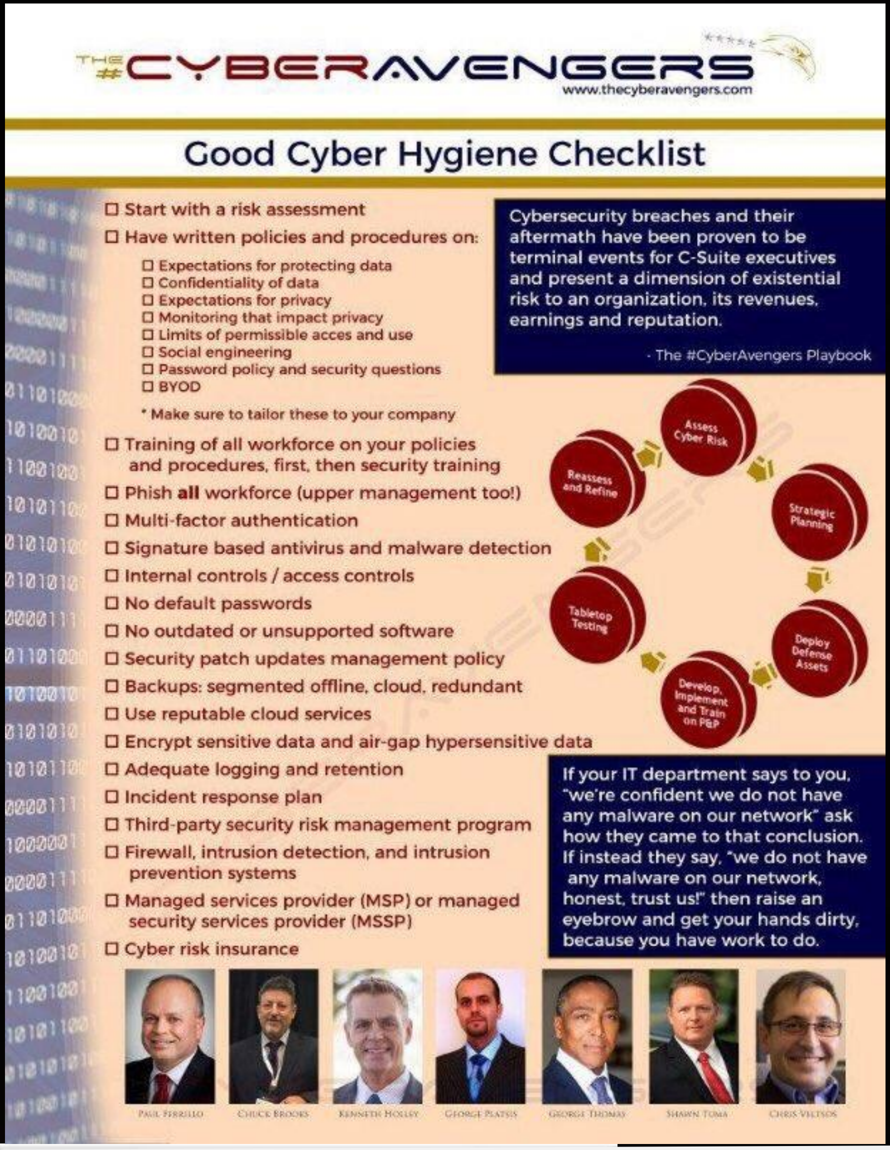
About the Poster

This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Matys, GM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berra, Saint Louis University - Sorina Dunose, Ubisoft Divertissements Inc - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, skWorks - Vaman Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

Source: https://securingthehuman.com/resources/posters

General Internet User Safety Tips



THE #CYBERAVENGERS
www.thecyberavengers.com

Good Cyber Hygiene Checklist

- ☐ Start with a risk assessment
- ☐ Have written policies and procedures on:
  - ☐ Expectations for protecting data
  - ☐ Confidentiality of data
  - ☐ Expectations for privacy
  - ☐ Monitoring that impact privacy
  - ☐ Limits of permissible acces and use
  - ☐ Social engineering
  - ☐ Password policy and security questions
  - ☐ BYOD

  * Make sure to tailor these to your company
- ☐ Training of all workforce on your policies and procedures, first, then security training
- ☐ Phish **all** workforce (upper management too!)
- ☐ Multi-factor authentication
- ☐ Signature based antivirus and malware detection
- ☐ Internal controls / access controls
- ☐ No default passwords
- ☐ No outdated or unsupported software
- ☐ Security patch updates management policy
- ☐ Backups: segmented offline, cloud, redundant
- ☐ Use reputable cloud services
- ☐ Encrypt sensitive data and air-gap hypersensitive data
- ☐ Adequate logging and retention
- ☐ Incident response plan
- ☐ Third-party security risk management program
- ☐ Firewall, intrusion detection, and intrusion prevention systems
- ☐ Managed services provider (MSP) or managed security services provider (MSSP)
- ☐ Cyber risk insurance

> Cybersecurity breaches and their aftermath have been proven to be terminal events for C-Suite executives and present a dimension of existential risk to an organization, its revenues, earnings and reputation.
>
> - The #CyberAvengers Playbook

> If your IT department says to you, "we're confident we do not have any malware on our network" ask how they came to that conclusion. If instead they say, "we do not have any malware on our network, honest, trust us!" then raise an eyebrow and get your hands dirty, because you have work to do.

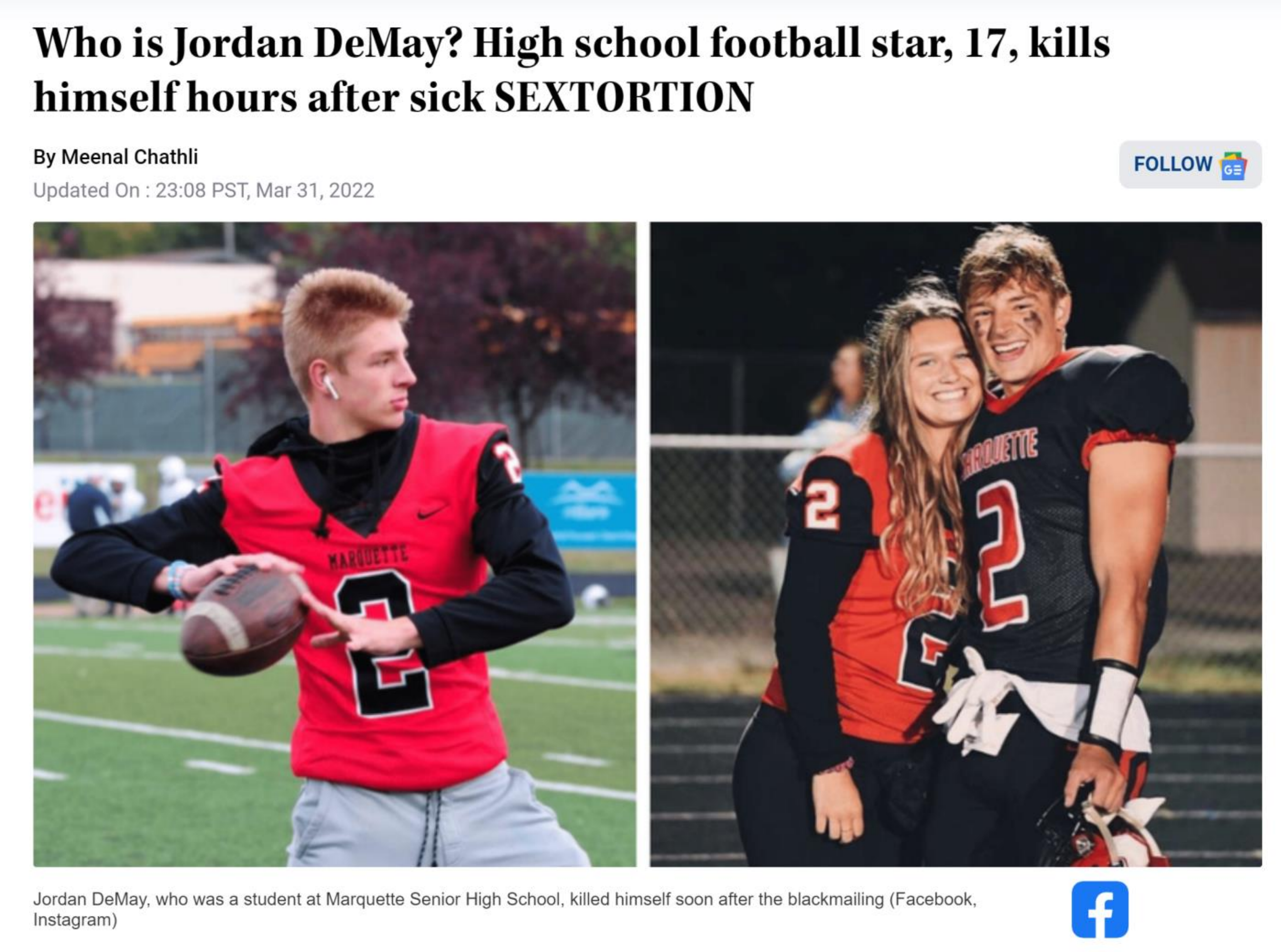
Paul Ferrillo · Chuck Brooks · Kenneth Holley · George Platsis · George Thomas · Shawn Tuma · Chris Veltsos

Source: https://thecyberavengers.com

Conclusion

- Sextortion is a serious Crime.
- It is becoming more common than people realize.
- Payment by Cryptocurrency makes it easy for Sextortionists to obtain money from naive people.
- Save the information.
- Do NOT PAY the money to appease the Sextortionist.
- Contact Law Enforcement if possible.
- Cover your webcam.

In Memory of Jordan DeMay



Who is Jordan DeMay? High school football star, 17, kills himself hours after sick SEXTORTION

By Meenal Chathli

Updated On : 23:08 PST, Mar 31, 2022

Jordan DeMay, who was a student at Marquette Senior High School, killed himself soon after the blackmailing (Facebook, Instagram)

Source: https://meaww.com/jordan-demay-high-school-student-17-kills-himself-victim-to-online-sextortion

Thank You!

Questions & Answers

?

William Favre Slater, III

- President / CEO / CISO of
  Slater Tecchnologies, Inc
- 312-342-2626
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America

William Favre Slater, III

References and Resources

- Chathli, M. (2022). "Who is Jordan DeMay? High school football star, 17, kills himself hours after sick SEXTORTION". An article published March 31, 2022 at MEAWW.com.
- Retrieved from https://meaww.com/jordan-demay-high-school-student-17-kills-himself-victim-to-online-sextortion.
- eDiscovery Today. (2023). What Happens Every 60 Seconds on the Internet. Retrieved from https://ediscoverytoday.com/.
- eSafety. (2023). Sextortion Safety Poster. Retrieved from https://safety.gov.au .
- Hall, J. (2023) "Three Nigerians Charged In Sextortion Connected To Marquette Teen's Suicide". Published at Radio Results Network. May 3, 2023. Retrieved from
- https://www.radioresultsnetwork.com/2023/05/03/breaking-three-nigerians-charged-in-sextorton-connected-to-marquette-teens-suicide/ .
- Kaass Law. (2023). What Is Sextortion Under California Law. Retrieved from https://kaass.com/what-is-sextortion-under-california-law/
- Olusesi, C. (2023) "Three Nigerian Nationals Await Extradition To U.S. For Sexual Extortion That Led 17-Year-Old Boy To Commit Suicide" Published May 4, 2023 at Information Nigeria.
- Retrieved from https://www.informationng.com/2023/05/three-nigerian-nationals-await-extradition-to-u-s-for-sexual-extortion-that-led-17-year-old-boy-to-commit-suicide.html.
- SANS Institute. (2019). Creating a Cyber Secure Home. Retrieved from https://www.sans.org/newsletters/ouch/creating-a-cybersecure-home/.
- Slater, W. F. (2018) . How to Be Anonymous Online. Retrieved from https://billslater.com/writing/beanonymous.pdf.
- Slater, W. F. (2023). Sextortion: What You Need to Know. Retrieved from https://billslater.com/writing/sextortion2023.pdf.
- Statista. (2023). Cybercrime Expected to Skyrocket in the Coming Years. Retrieved from https://www.statista.com/outlook/technology-outlook.
- The Cyberavengers. 2023. Good Cyber Hygiene Checklist. Retrieved from https://thecyberavengers.com .
- Visual Capitalist. (2023) . Global Economy. Retrieved from https://www.visualcapitalist.com/.

I have learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel.

Maya Angelou
1928-2014

Photo by Michael Collopy