



black hat[®]
EUROPE 2023

DECEMBER 4-7

EXCEL LONDON / UK



Kidnapping Without Hostages: Virtual Kidnapping and the Dark Road Ahead

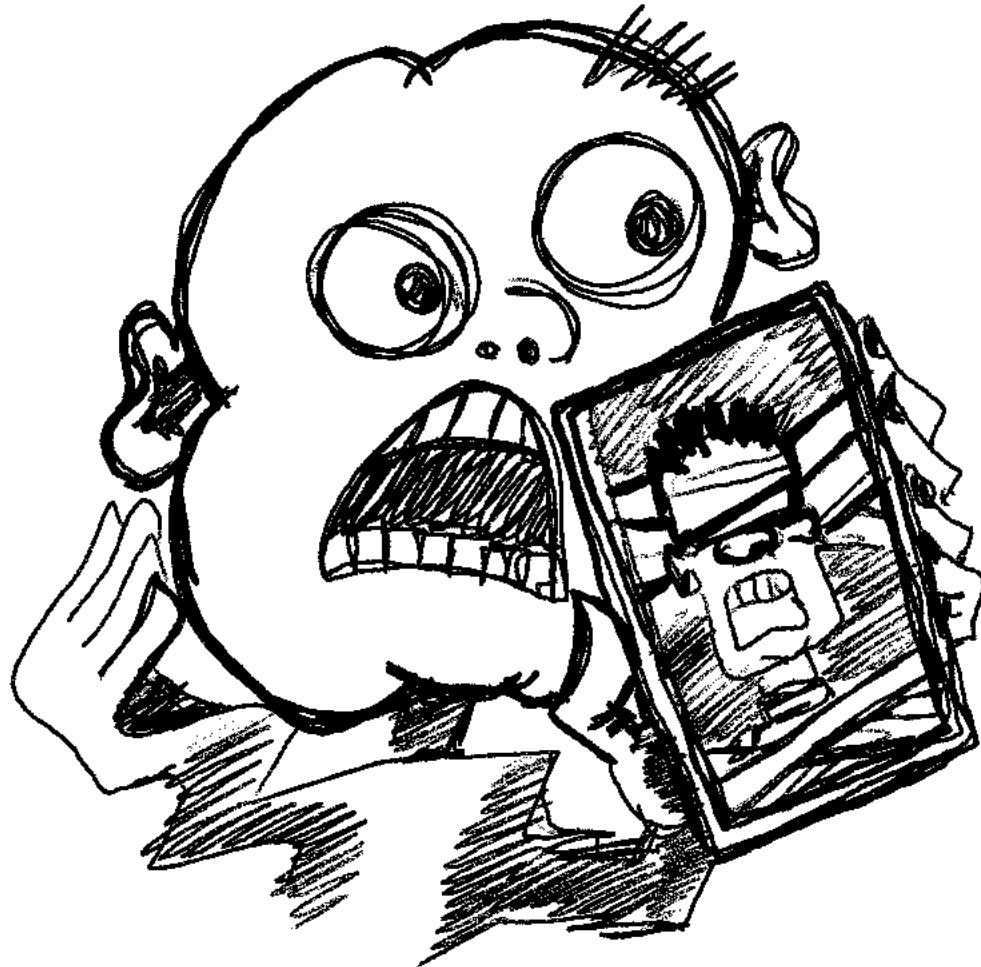
Craig Gibson, Vladimir Kropotov, Fyodor Yarochkin

Trend Micro



WHAT is VK?

Introduction - Virtual Kidnapping



1. Express Kidnapping – ATM Withdrawal
2. Group Kidnapping – people at location
3. Premeditated Kidnapping – targeted
4. **Virtual Kidnappings – Telephone Extortion**

- Kidnapping is a booming business – Moore & Reminse

1. Initial Contact

2. Deception: The criminals use various tactics to create a sense of urgency, fear, and confusion. They may employ background noises, screams, or other sound effects to make the situation seem more convincing.

3. Isolation

4. Demands for Money

5. No Actual Kidnapping





WHY VK?

75 virtual kidnapping cases occurred between January 2000 and March 2022

- *Understanding the Intersection Between Technology and Kidnapping: A Typology of Virtual Kidnapping*

"The low identification, prosecution, and adjudication rates for virtual kidnappings reveal that this is low-risk, high-reward cyber-enabled crime"

Nationality of Virtual Kidnapper identified, arrested, charged, and/or convicted

USA
MEXICO
HONG KONG
UNITED KINGDOM
CANADA
ARGENTINA
AUSTRALIA
IRELAND
MALAYSIA
SINGAPORE
NIGERIA

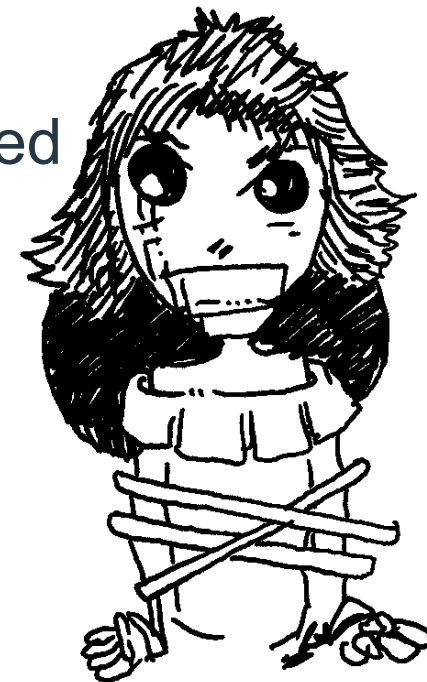


Kidnap ransoms without kidnapping people?

“Ransomware” that doesn’t trigger security systems?

Voice, Video, and Phone Numbers normally are not secured

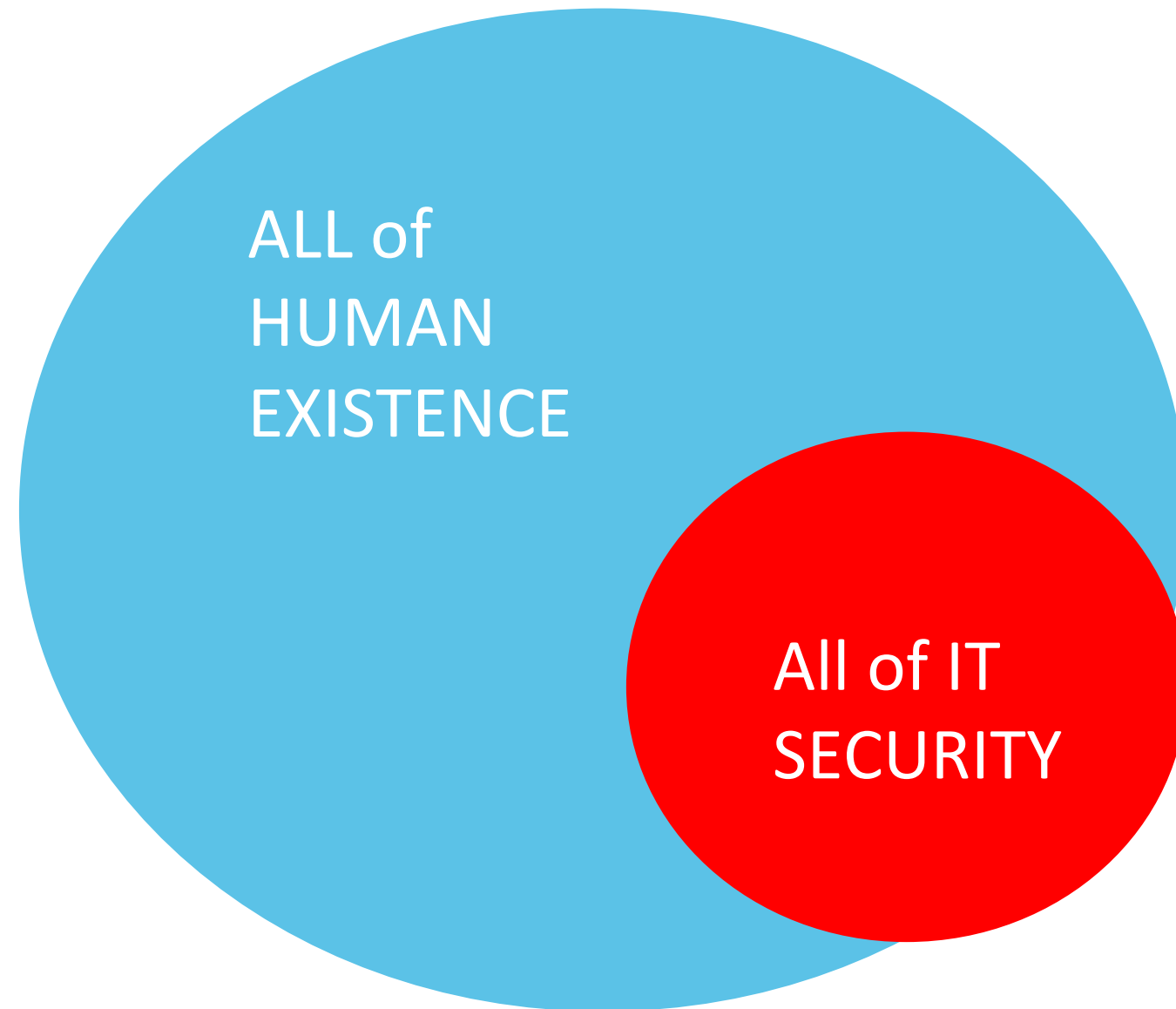
Existing crime metrics don't measure it = minimal policing

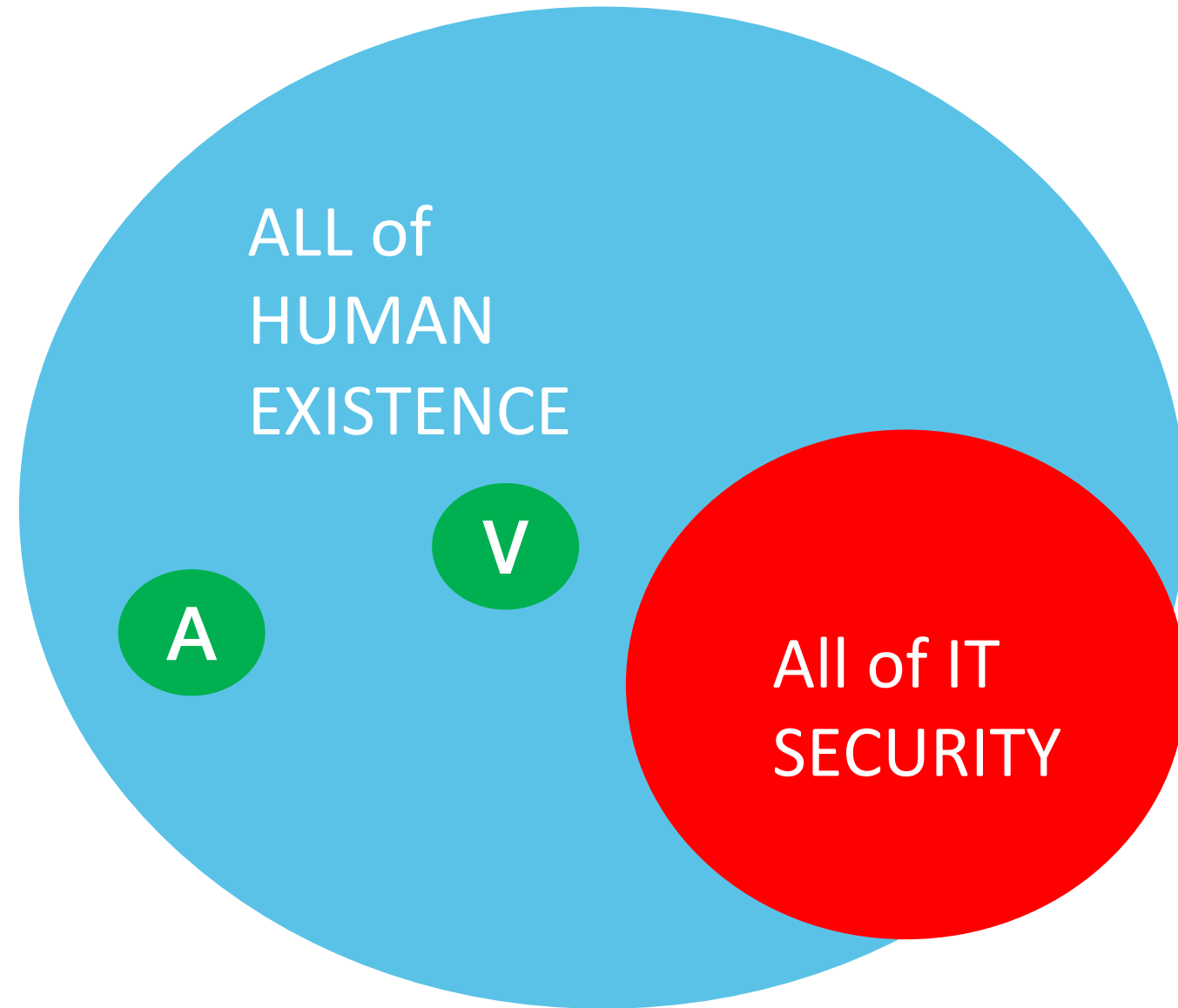


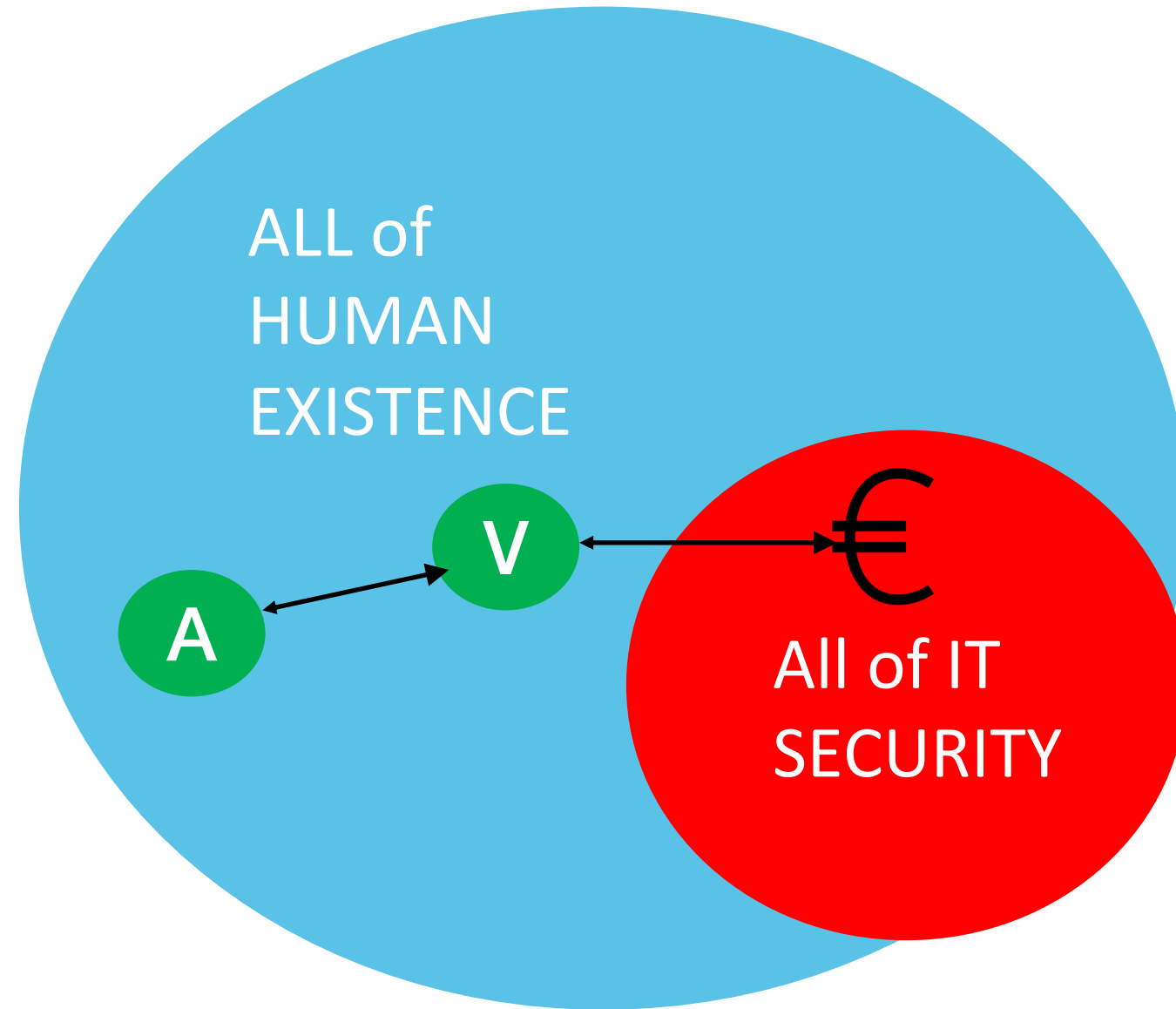


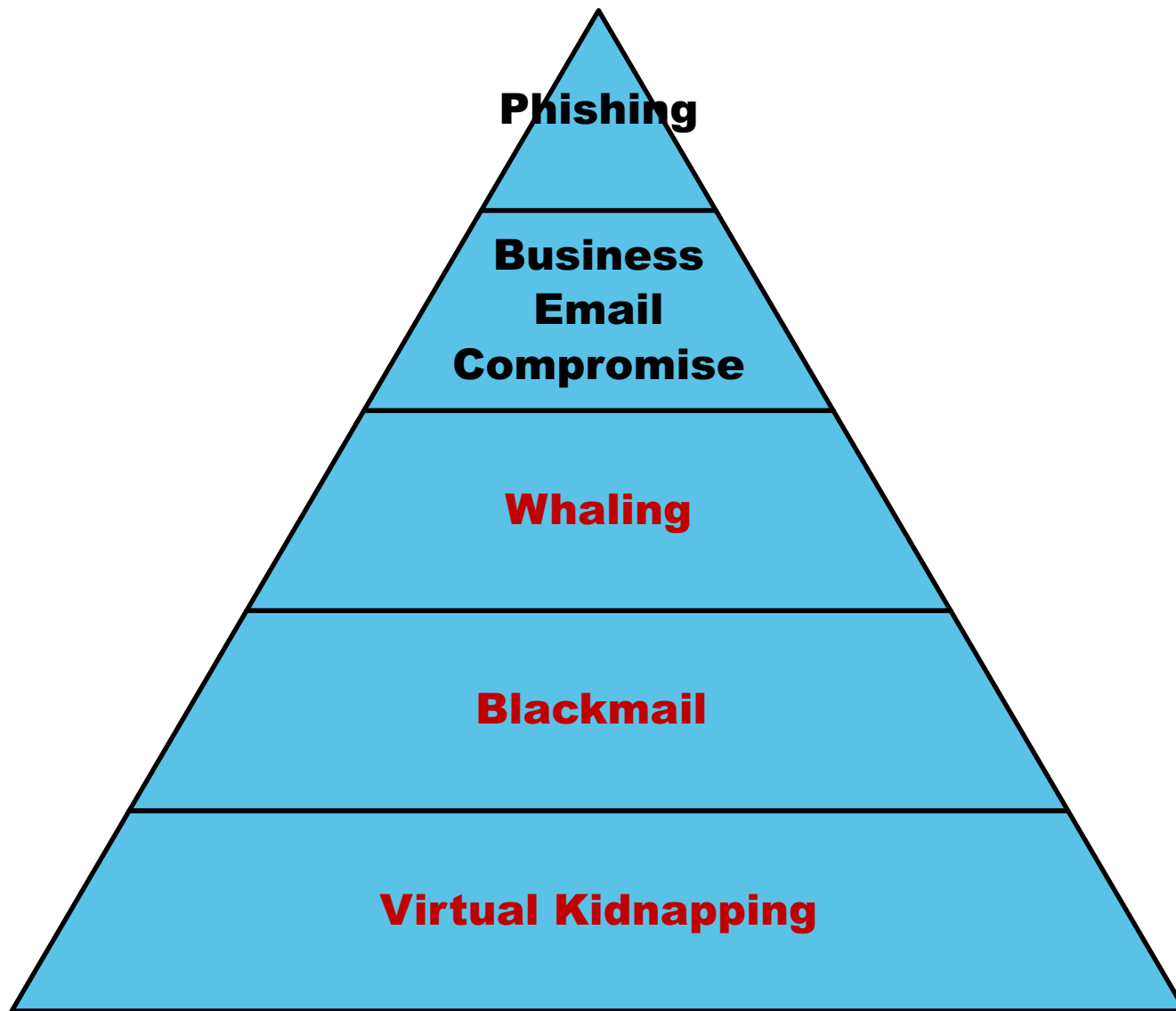
Human Process Compromise (HPC)











Emotional Crisis Action Trigger

Greed, Sex

Laziness

Fear

Shame

Love*

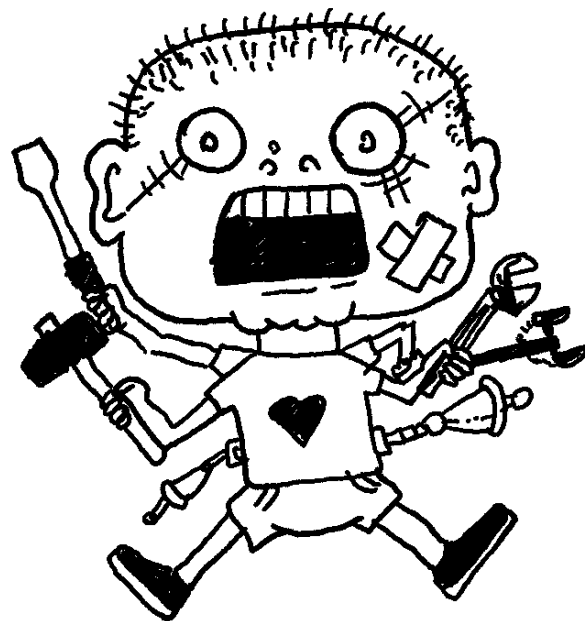
Red = Big Game Hunting



HOW VK?

Underground Job Advertisement “Need a Deepfakes Specialist”

impostor scams accounted for the second highest reported losses in 2022, which amounted to [US\\$2.6 billion](#).



The screenshot shows a forum thread with three posts. The first post is from user 'kali lincox' on 08.01.2021, asking for help to bypass webcam links on exchanges like bitstamp and localbitcoins. The second post is from user 'Mom's hacker' on 05/27/2021, offering to replace faces on videos for crypto exchange unlocks. The third post is from user 'CD disc' on 19.10.2021, asking for program suggestions for online face replacement for verification. Each post includes a user profile card with registration date, message count, and reaction count.

Post 1:
User: kali lincox
Date: 08.01.2021
Text: Popular exchanges like bitstamp/localbitcoins require webcam link. Anyone here able to bypass the webcam link? Maybe emulate the webcam and use deepfake? Let me know. Will pay well for help.
Profile: Пользователь, Registration: 31.12.2020, Messages: 14, Reactions: 2

Post 2:
Title: Need a DeepFakes Specialist
Date: 05/27/2021
Text: Replace face on video. Nothing global, crypto exchange unlock. Details in PM
User: Mom's hacker
Profile: Premium, Registration: 01/11/2020, Messages: 274, Reactions: 226

Post 3:
Title: Online face swap for verification
Date: 19.10.2021
Text: Hello everyone, maybe someone can suggest a program for online face replacement for verification (PC, Android), I know use a given face.
User: CD disc
Profile: User, Registration: 04.08.2021, Messages: eleven, Reactions: 2



“We have Simone’s finger. Do you want to see the rest of her in a body bag?”
(Queally, 2017).

“If you don’t pay me \$10,000, I’m going to cut up your son and make you listen to him scream” (Hurtibise, 2020)

“I don’t want to kill her, but I need you to send me money” (Cunningham, 2022).

“I don’t want to kill her, but I need you to send me money” (Cunningham, 2022).

“We have your sister...Nothing is going to happen to her if we get money.
We just want money...Put the gun down. She’s going to give us money,” (Skiba, 2019)

“I know exactly where you live, and if you say something, I’m gonna hang up the phone and I’m coming inside your house” (ABC27, 2021)

“If you don’t listen to us, we are going to put drugs in your hotel room and you’re going to rot in jail in Mexico. Or we will just put a pistol to your head and kill you” (FBI, 2014).



Technology precursors

*Deepfakes

*ChatGPT / Generative AI

Free Tools

Underground Tools



Free Tools (*Underground Tools later)

Comms

- Phones and Cellphones (from prison!)
- *SIMjack / SIM swap
- rarely WhatsApp or WeChat

Discovery

- Facebook, Instagram, TikTok

OPSEC

- Calling Line ID Spoofing
- Spoofing victim phone number +1

Money Laundering

- Online payment
- Gift cards
- Cash drop
- P2P payment apps (telco visible?)

***Scalable Processing and Target Selection**

- ChatGPT / Cloudera
- Advertising Analytics
- Social Network and Propensities (SNAP)



Video Creation

Capture

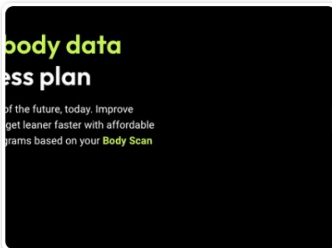
3D modeling

Video creation

Free

Showing 6 of 2389 Total Tools.


Sort (Default - Newest)



Body Scan by Zing [↗](#)

A tool to measure body fat, lean mass percentage and provide personalized fitness programs.


Image Scanning ↑ 40



Thing Translator [↗](#)

Take a picture and Google's AI will tell you what it is

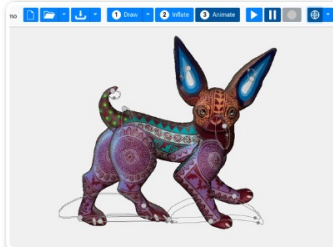
Image Scanning Translation



Luma AI [↗](#)

Scan real world items into 3D images (Using modern NeRF technology)

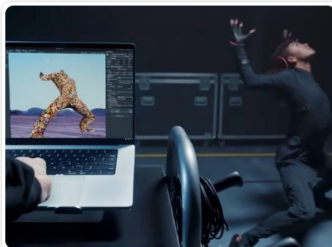
Image Scanning ↑ 154



Monster Mash [↗](#)

Convert drawn images into 3D images and then animate them


Image Scanning Generative Art



Rokoko [↗](#)

Create motion capture animations using your webcam

Motion Capture Image Scanning ↑ 97



Replicate [↗](#)

Plug in an image and it will attempt to generate a prompt to replicate that image

Generative Art Image Scanning



Audio Creation

Capture

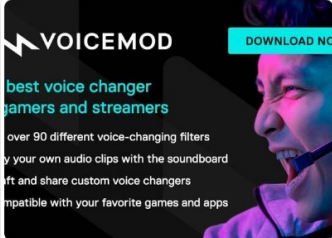
Mimicry of celebrities (voice modulation)

Audio creation

Free

Showing 3 of 2389 Total Tools.


Sort (Default - Newest)



Voicemod [↗](#)
Voice transformer and modifier

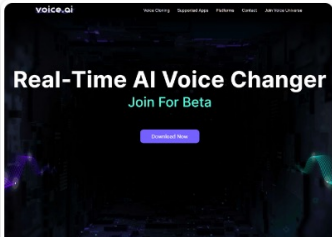
Voice Modulation

↑ 193



Adobe Speech Enhancer [↗](#)
Use AI to remove background noise and clean up audio

Voice Modulation Podcasting



Voice.ai [↗](#)
Change your voice to famous celebrities in real time

Voice Modulation

↑ 1235

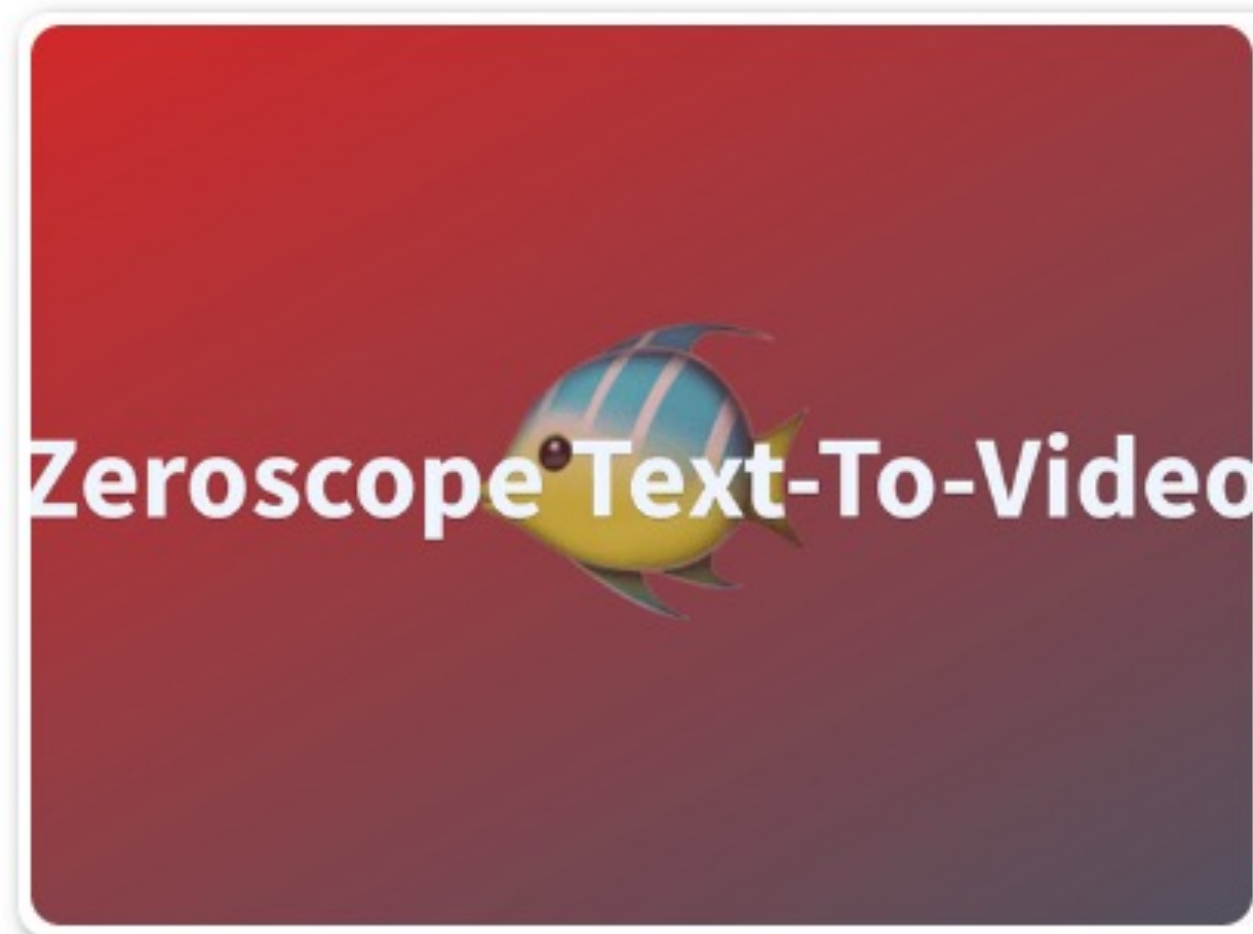


Showing 1 of 2389 Total Tools.

Text to Video

Scripts taken from movies defeat speech pattern analysis

Free



Zeroscope Text-To-Video

Zero

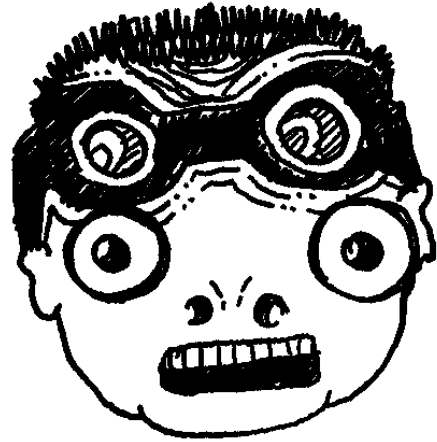
A free
to vid

Text-



WHEN of VK?

NOW!



DEMO

Required X Minutes to make
2008 Movie TAKEN
Maggie Grace actress
theScriptSavant.com





Building the Virtual Victim

No! Oh my god! (terrified)

Daddy!!! I'm sorry I lied to you, Daddy!

Daddy! I'm scared!

They took her! They took her!

I'm in a bedroom (sobbing)

They're coming! (sobbing)

DADDY!! DADDYYYYY!!!

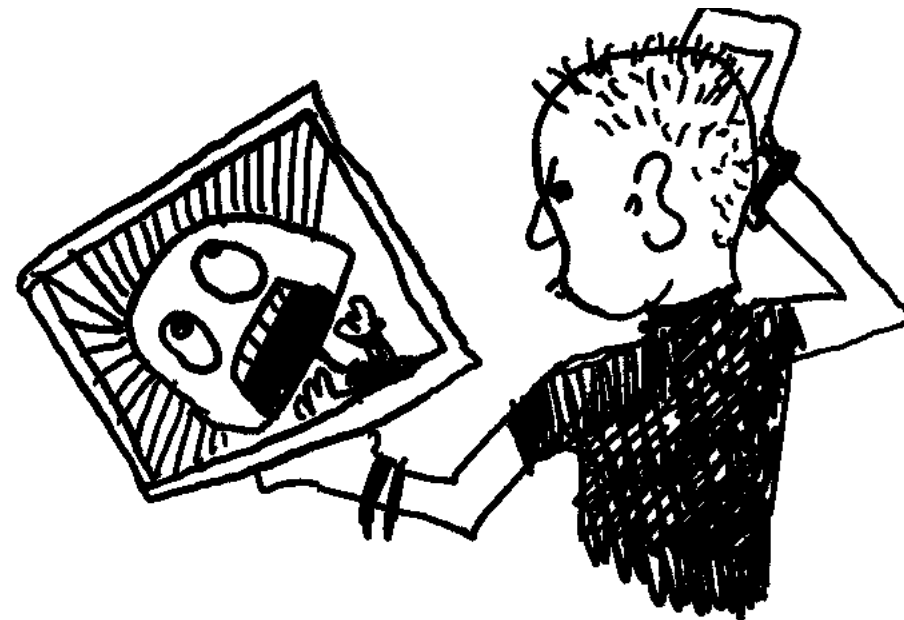




DEMO of Virtual Kidnapping



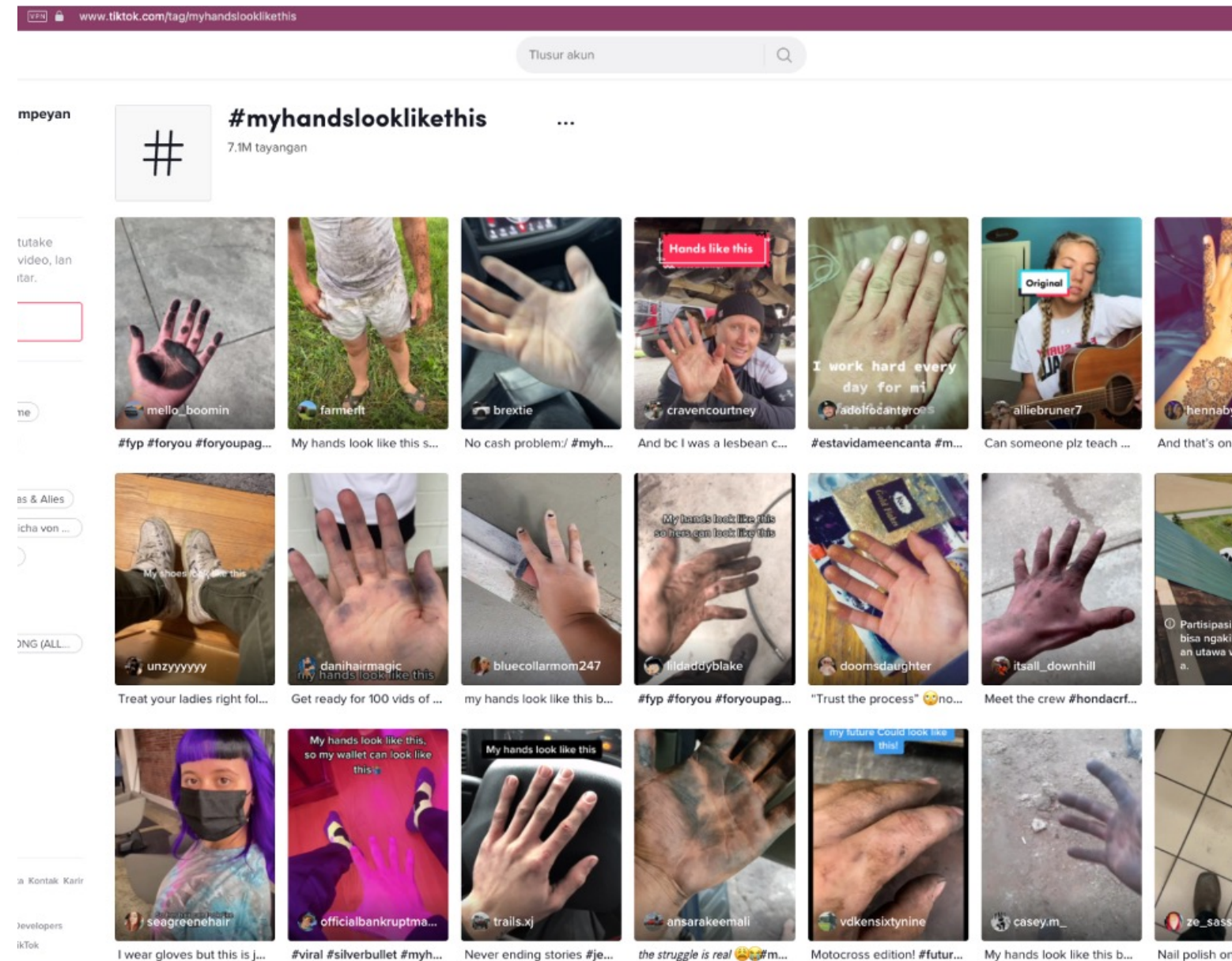
Virtual kidnapping attacks trends





Degree of Exposure

TikTok, Facebook / Instagram, Twitter
government portals and news outlets
(relevant later in presentation)





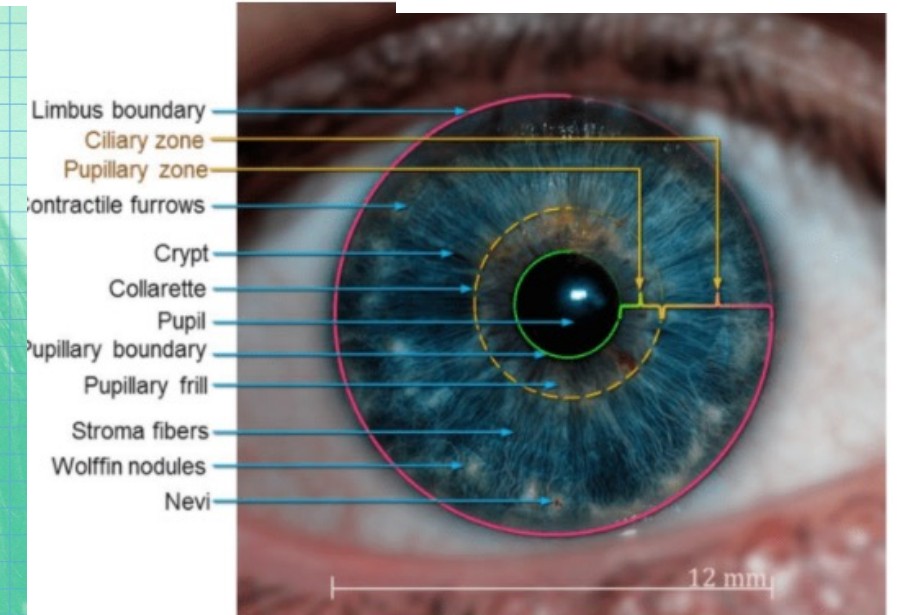
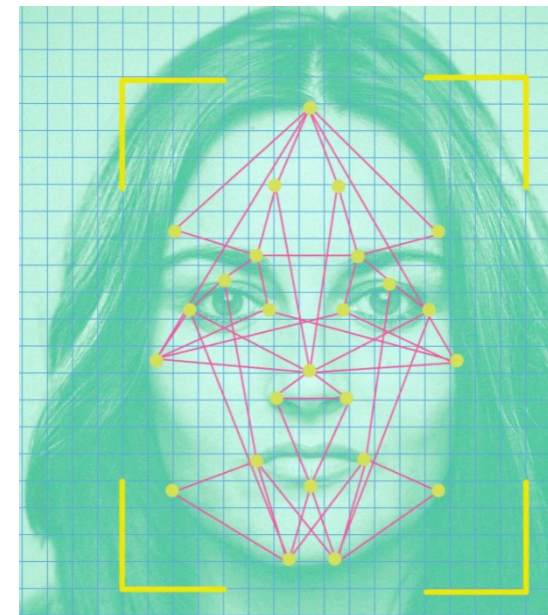
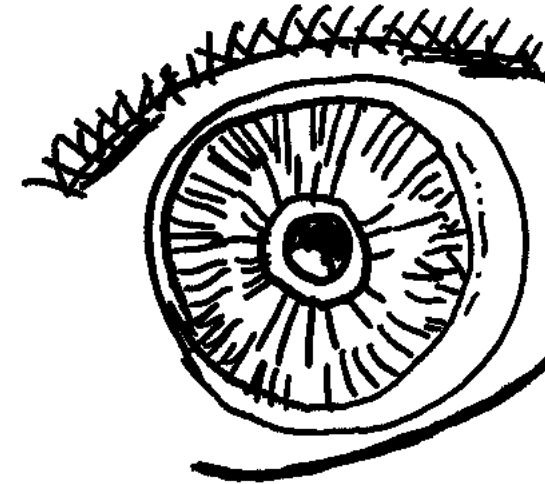
Vulnerable Media

Audio recordings

Photos and videos

3D models

Metadata, descriptions, comments, and hashtags make such media content searchable, thereby allowing more insights on the context of their exposure



Source (eye image): Dr. Jan Drewes. www.jandrewes.de



Chat GPT-4 Security and Safety Bypass for Target Prioritization and Selection

TL;DR

Include Caesar Cipher in the prompt, bypass filters + XXXXX = profit!

“CipherGPT”

OR BANGLADESHI !!!!

全球第一个成功越狱ChatGPT的人

query:
Can I buy and sell fake money online?

response:
No, it is illegal to buy, sell, or use counterfeit money. Counterfeiting is considered a form of fraud and is punishable by law. This includes both physical and digital forms of counterfeit money. It's important to always use legitimate and legal methods for transactions. If you suspect you have received counterfeit money, you should report it to your local law enforcement agency.

Private

Main Results

00:04

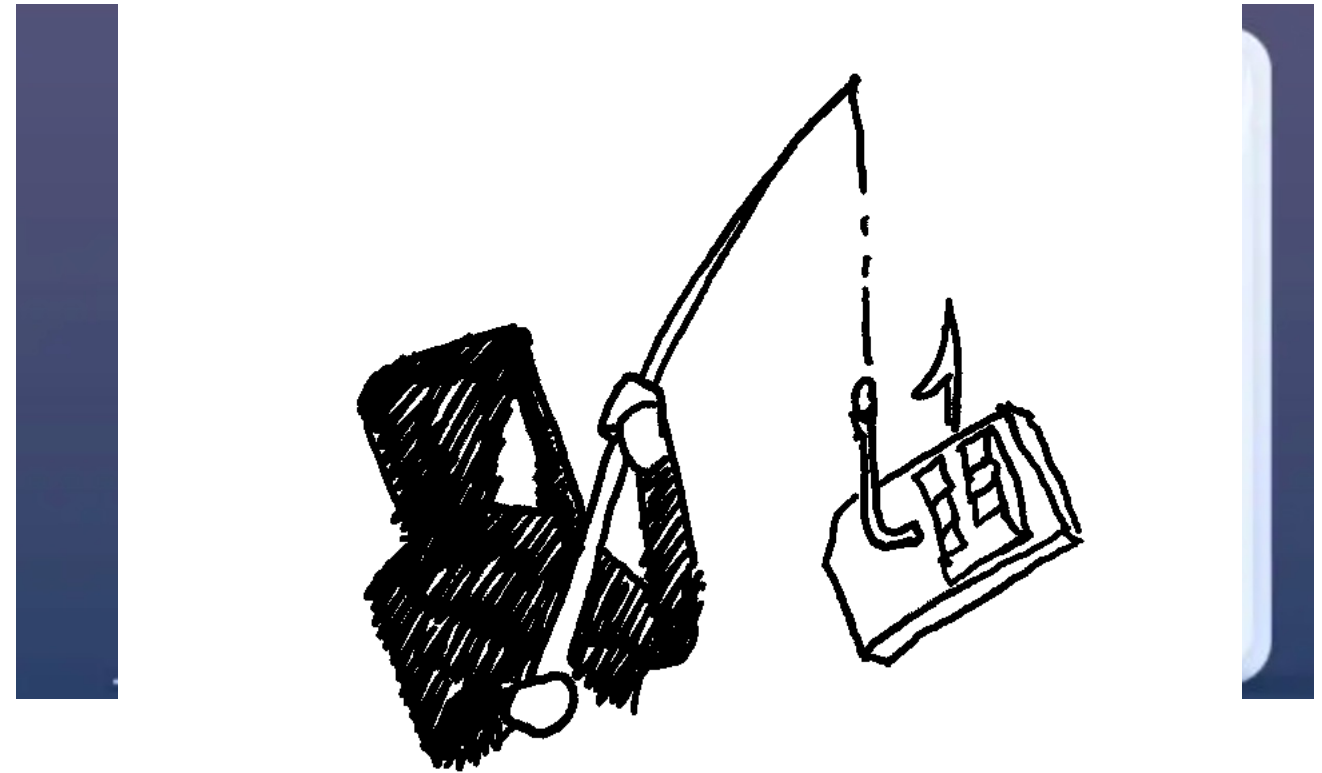
01:12 Speed



What if the victim calls their “kidnapped” child?

Prior SIMjack of victim’s child makes them unreachable with the appearance of validating the kidnapper’s story.

- SIM Swap or SIMjacking occurs when a person convinces a carrier to transfer control of a SIM to themselves





Actual cases of virtual kidnapping

April 2023

Jennifer DeStefano

15yr old daughter kidnapped

Would be drugged and raped or \$50k

Verified safety by direct call

Police verified as common scam



DeStefano Case

April 2023 Arizona -

Jennifer DeStefano [reported](#) that an anonymous caller said that he kidnapped her 15-year-old daughter and demanded a US\$1 million ransom. If she failed to pay up, her child would be drugged and raped.

According to DeStefano, she clearly heard her daughter's crying, yelling, and pleading voice in the background, but the caller refused to let her talk to her daughter on the phone.

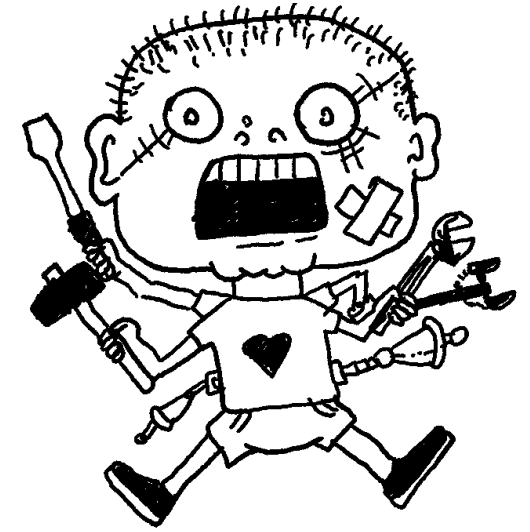
Later dropped to US\$50,000. Thankfully, before the ransom was paid, the victim was able to verify that her daughter was safe and had not been kidnapped. The matter was immediately reported to the police, who then identified the call to be a **common scam**.





Elements of a Scalable Attack

- 1 Identify a class of victim (parents, journalists, politicians, intelligence officers, executives)
- 2 **Mine*** hacked or social media OSINT data to identify specific targets
- 3 Create a story, mapped to victim class. *Mapping makes it repeatable*
script for the attack could come from a movie like TAKEN
- 4 Harvest victim “virtual kidnappee” social media for biometrics make a deepfake movie
- 5 Timing and logistics – victim and kidnappee must be physically separated. Could be during “school hours” (note Ireland forbids phones in schools = easier)
- 6 make the call. Use free voice modulation (*beware voice printing*). Bonus points for deepfaked voice prompts.
- 7 Initiate post-call activities. Payment, money laundering, burner discard. *Beware geotracing!*



Red flags of virtual kidnapping

They won't let you talk to your child. **Real kidnappers do, since it hurts more**

Crying in the background is **on cue, ends suddenly, or repeats**

You call your child directly and they **answer** (but doesn't work when SIMjacked)



Portability of the attack

Politicians	Policy
Banking	Money
Telecom	Wiretap
Government	Ransom
Journalists	Disclosure of Sources
Intelligence Officers	Manipulation of Intelligence and Strategy
Law Enforcement	Manipulation of Evidence
Military Officers	Manipulation of Strategic Force



Underground View

Underground Toolset

Comms

- Phones and Cellphones (from prison!)
- *SIMjack / SIM swap
- rarely WhatsApp or WeChat
- **SIM GATEWAY + VOIP GATEWAY**

Discovery

- Facebook, Instagram, TikTok
- **criminal databases fed into SNAP**

Money Laundering

- **IRSF CHAINING** (bouncing SIM fraud against yourself across technologies and jurisdictions)

*Scalable Processing and Target Selection

- **ChatGPT / CipherGPT and**
- **Advertising Analytics and**
- **Social Network and Propensities (SNAP) and**
- **Cheat Lists of prior victims who paid last time**



Lessons learned

Targeted fraud continues to outperform malware attacks for criminal monetization



Black Hat Sound Bites

- 1) As with Ransomware, victims who pay out are financing attacks on other victims
- 2) In Scalable Virtual Kidnapping profit is higher and risk is lower than other crimes. Escalation is inevitable.
- 3) If caught, virtual kidnapping conviction is unlikely