SAVING RYAN'S PRIVATES

Addressing the complex security problems around leaky nudes

Johnny Xmas, CISSP, GIAC
Technical Director of Training, GRIMM

Requisite Slide of Stuff you don't Care About

- Music Major
- Urban Explorer
- Crime Simulator
- Educator
- Community Leader
- **HACKER**

What did you just get Yourself Into?

- WHY the things we already know are critical
- Blind spots and lesser-understood attack vectors
- Reality check on what you can do

What did you just get Yourself Into?

- WHY the things we already know are critical
- Blind spots and lesser-understood attack vectors
- Reality check on what you can do


STATS!

STATS!

STATS!

I was gonna try to Google some stats,
so you just go do that.

It’s impossible to accurately
track this, anyway.

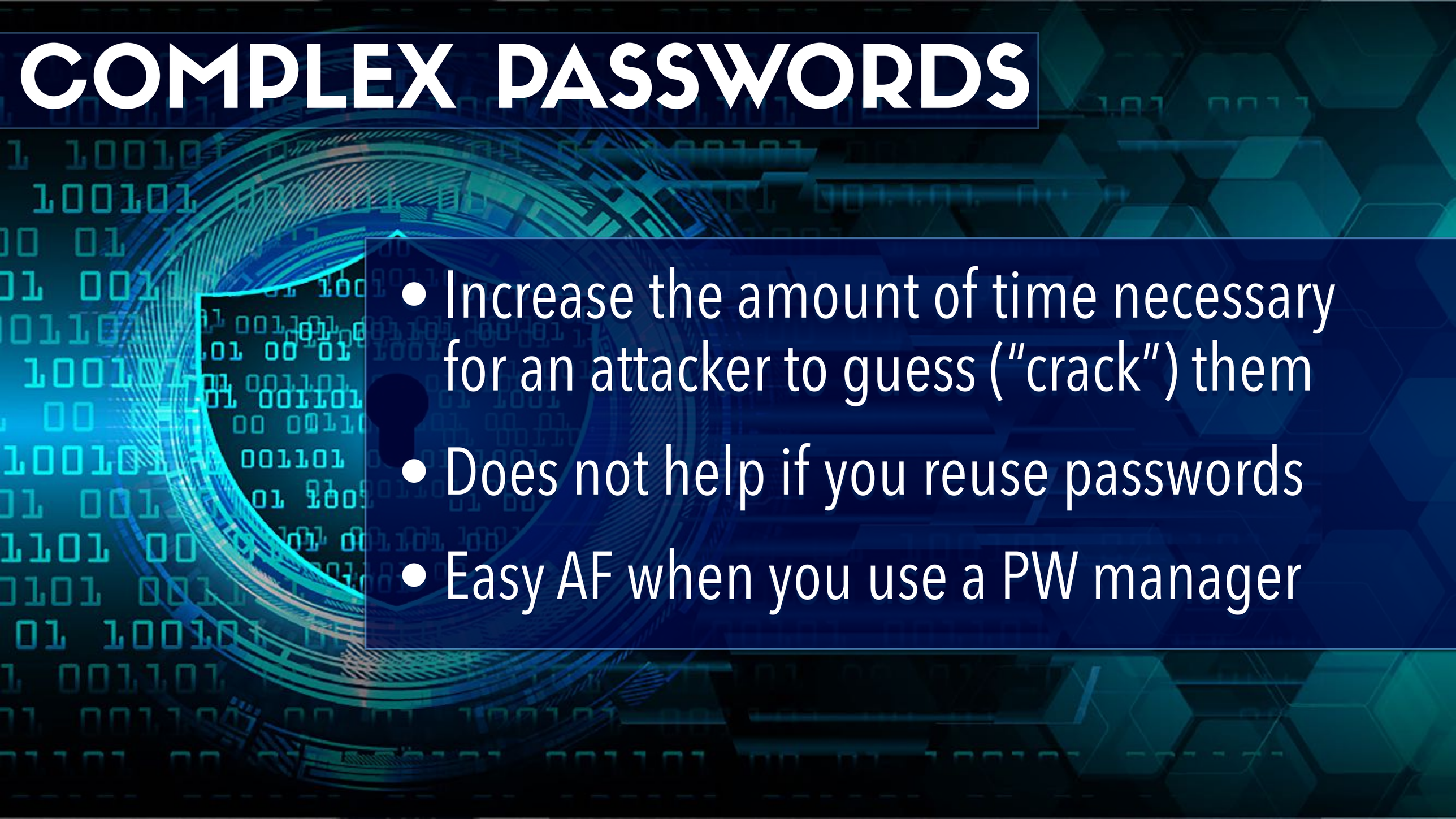
**WE ALL KNOW THIS IS
A HUGE PROBLEM.
YOU DON’T NEED THE STATS.**

QUIZ REVIEW!

UNIQUE PASSWORDS

- Billions of credentials are leaked/shared every year from hacked systems
  - Vendors rarely directly inform their users
- Attackers “spray” these credentials at OTHER sites & services

COMPLEX PASSWORDS



- Increase the amount of time necessary for an attacker to guess (“crack”) them
- Does not help if you reuse passwords
- Easy AF when you use a PW manager

Multi-Factor Auth.

- Like having 2 passwords, one of which rotates every few seconds
- Great even when your password sucks
- Requires attacker to access the device or service that has your “seed token”


So How do Leaks Happen, Then?

Your Partner Sucks
(In the bad way)

- Intentional Leaks
- Their cybersecurity posture sucks
- You're both using a non-encrypting messaging system
  - No End-to-End ("E2E") Encryption
  - No Message Expiration

Your Partner Sucks

(In the bad way)

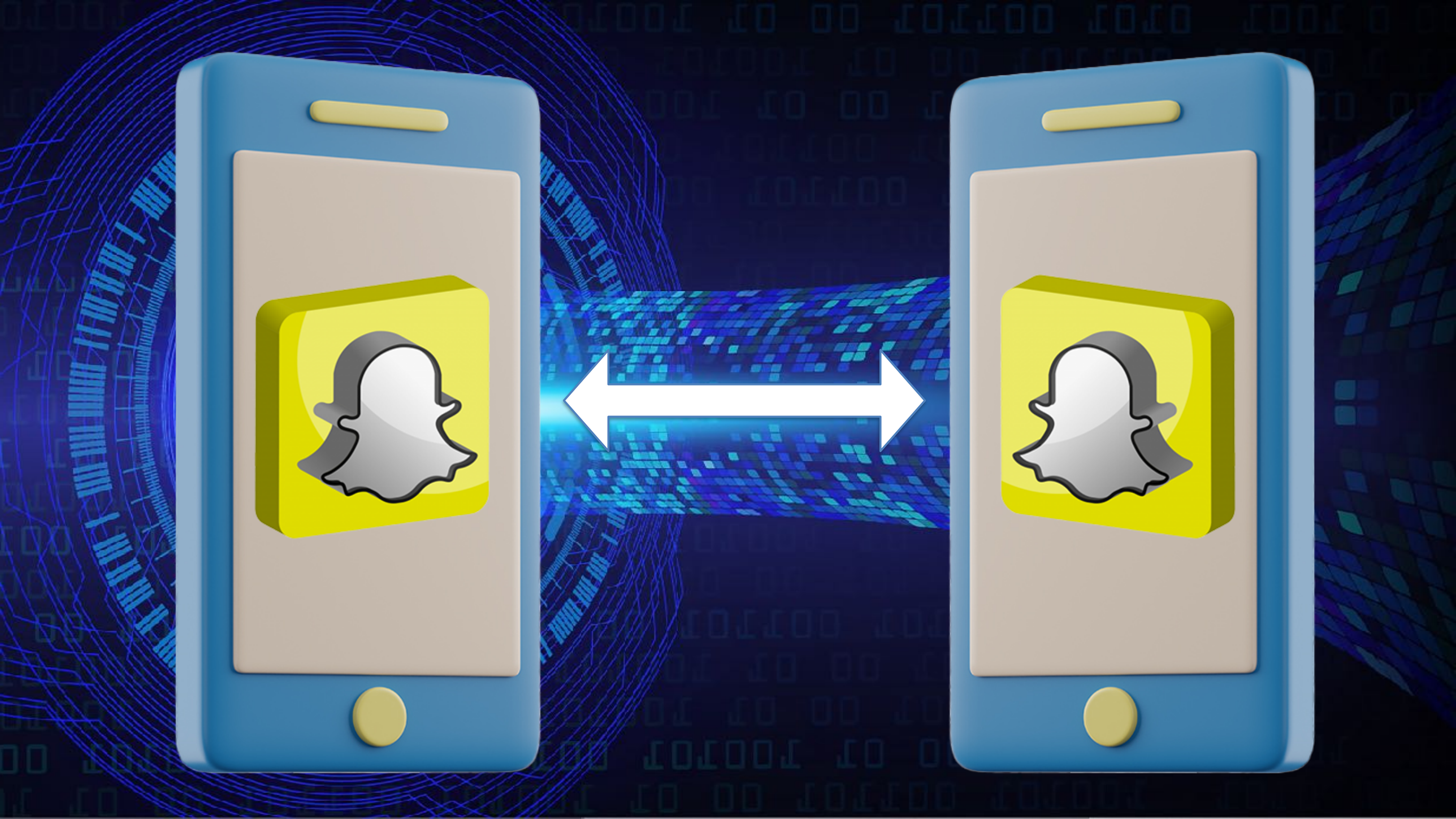
- Intentional Leaks
- Their cybersecurity posture sucks
- They're using a non-encrypting messaging system

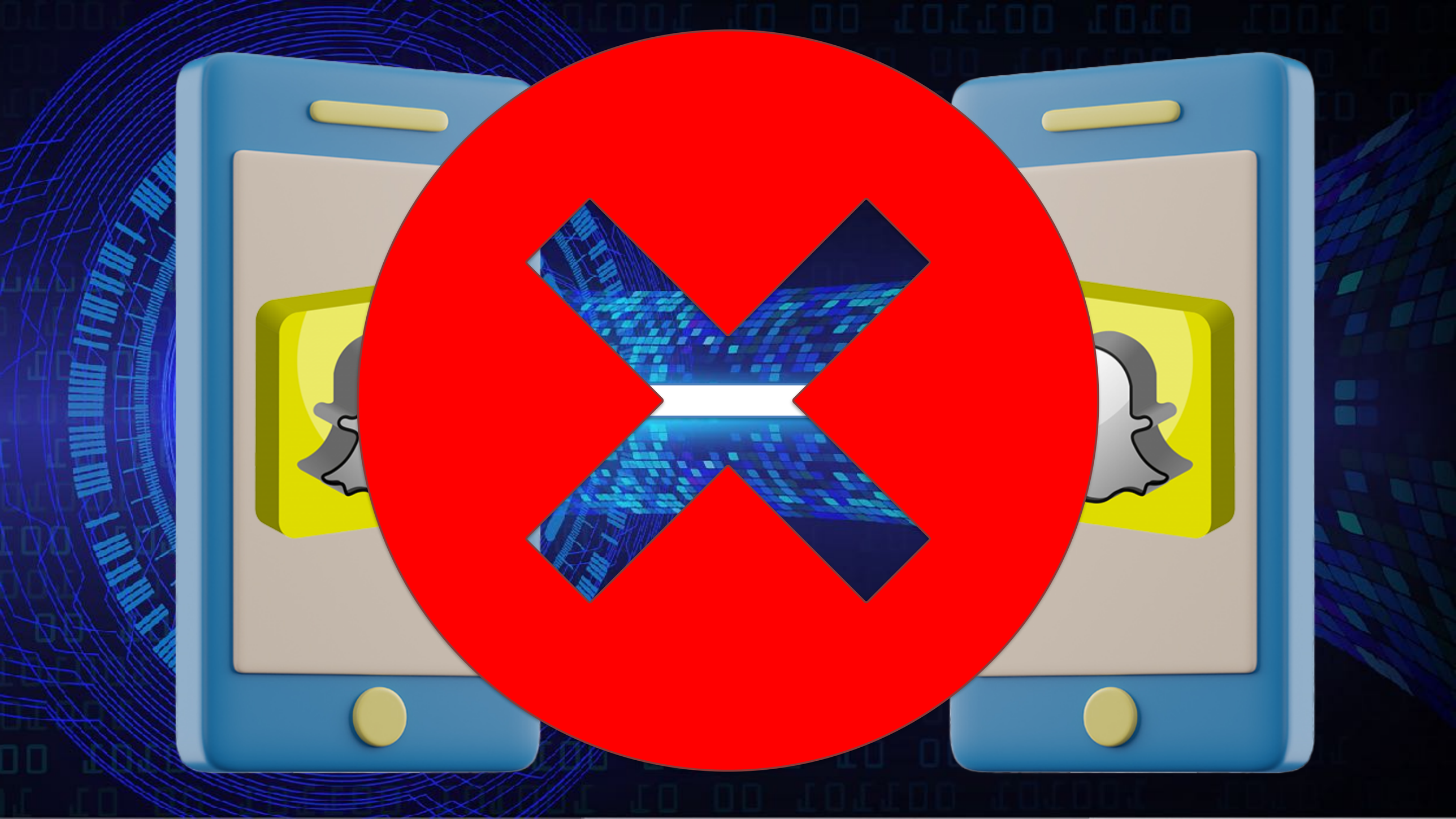
IT IS IMPOSSIBLE FOR ANY GROUP CHAT TO HAVE E2E ENCRYPTION.

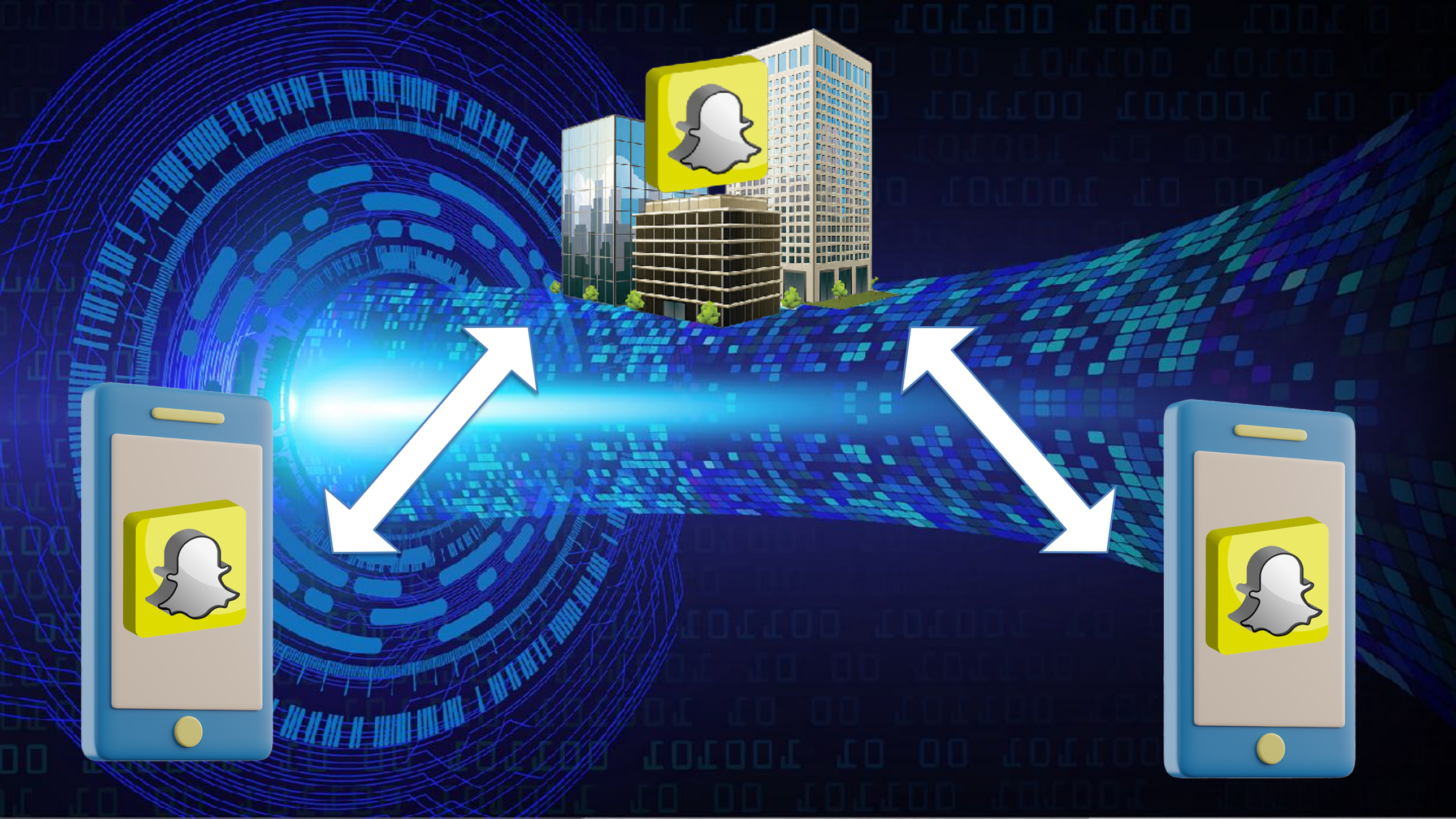
- No End-to-End Encryption
- No Message Expiration

You're Using Somebody Else's Computer

- You didn't know
- You do this constantly
- It's required for many (most) scenarios







MOTHERBOARD
TECH BY VICE

Snapchat Employees Abused Data Access to Spy on Users

Two former employees said multiple Snap employees abused their access to Snapchat user data several years ago. Those sources, as well as an additional two former employees, a current employee, and a cache of internal company emails obtained by Motherboard, described internal tools that allowed Snap employees at the time to access user data, including in some cases location information, their own saved Snaps and personal information such as phone numbers and email addresses. Snaps are photos or videos

- **A former member of Facebook's escalations team is suing the company.**
- **His lawsuit accuses Facebook of introducing a tool in 2019 to let staff access deleted Messenger data.**
- **The ex staffer says this data was sometimes shared with law enforcement.**

"It doesn't appear that Facebook had even the most basic compliance framework to safeguard access to user data," he said in his blog post. "It is entirely predictable that if app developers are not held to their promises about data collection and sharing, they might not be candid with Facebook about their intentions. Yet it seems that Facebook made no effort to establish the bona fides of developers, much less verify or audit what user data app developers actually harvested and shared."

You're Using Somebody Else's Computer

You're Using Somebody Else's Computer

The Fappening

Page Talk

From Simple English Wikipedia, the free encyclopedia

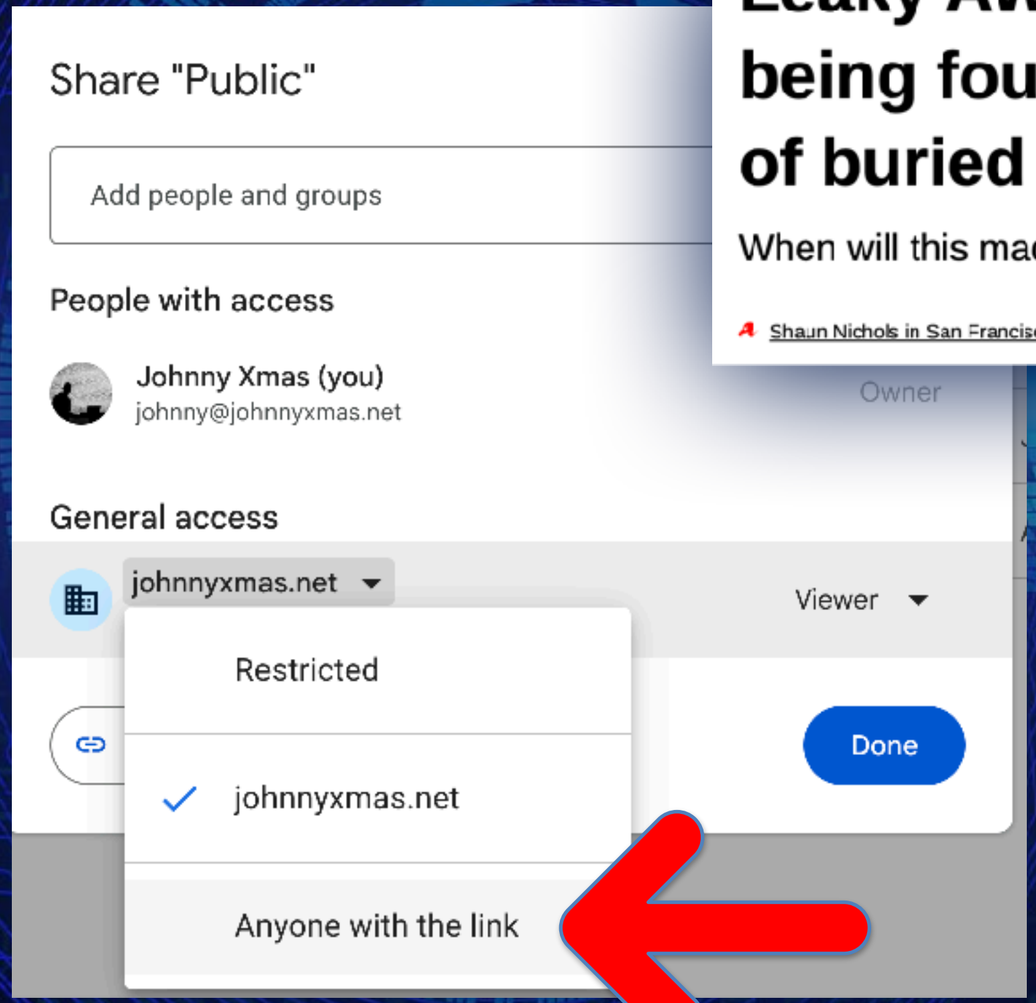
On August 31, 2014, a collection of almost 500 private pictures of many celebrities, mostly wom
imageboard 4chan, and later shared by other users on websites and social networks such as Im

The images were initially believed to have been obtained via a breach of Apple's cloud services
been gained via targeted phishing attacks.[1]

iCloud Drive

IT IS IMPOSSIBLE FOR ANY GROUP CHAT TO HAVE E2E ENCRYPTION.

LEAKY LINKS



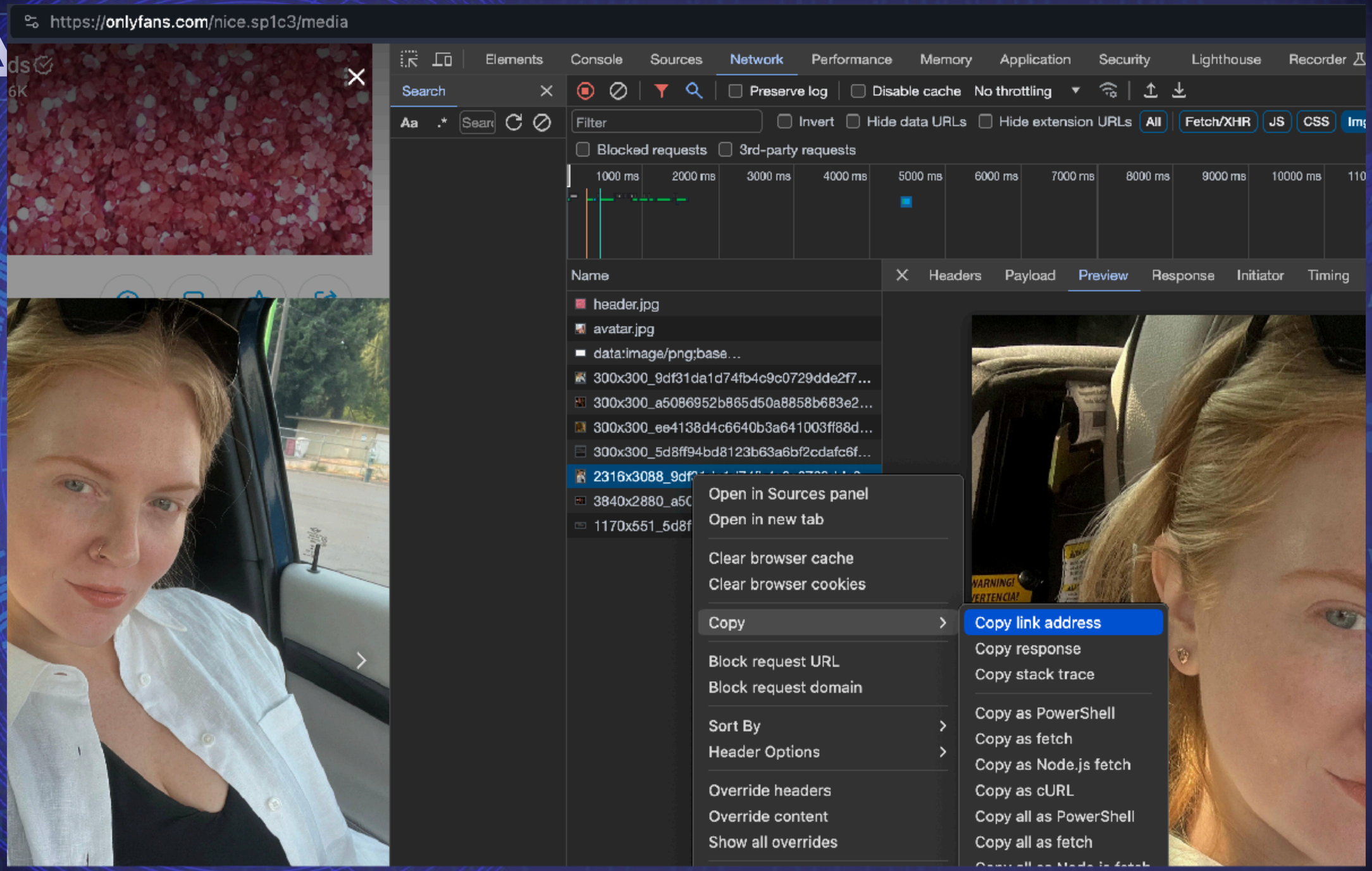
Leaky AWS S3 buckets are so common, they're being found by the thousands now – with lots of buried secrets

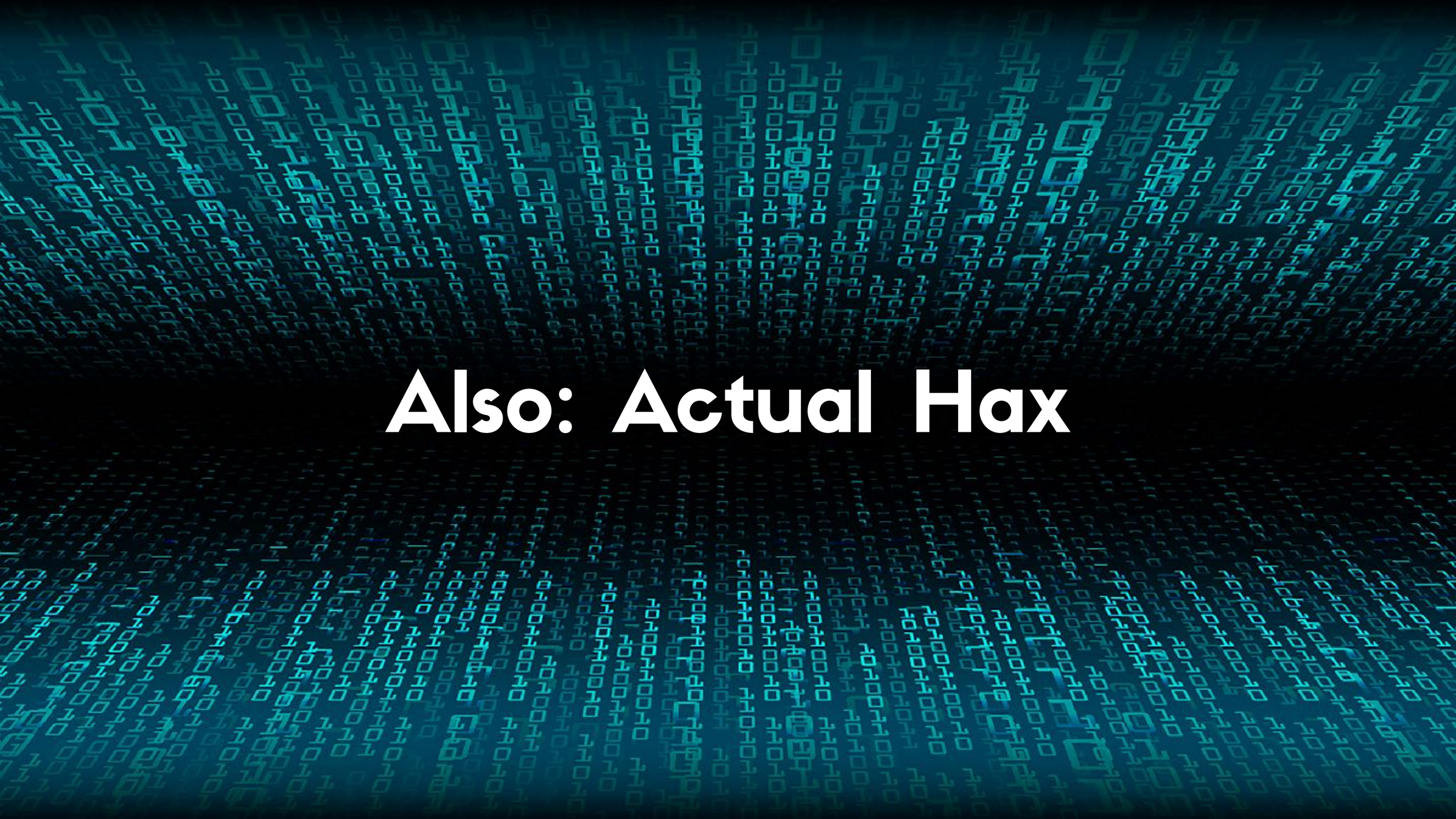
When will this madness end?

Shaun Nichols in San Francisco Mon 3 Aug 2020 // 23:47 UTC

Discord recently fixed this problem…

OnlyFans has it *RIGHT NOW.*

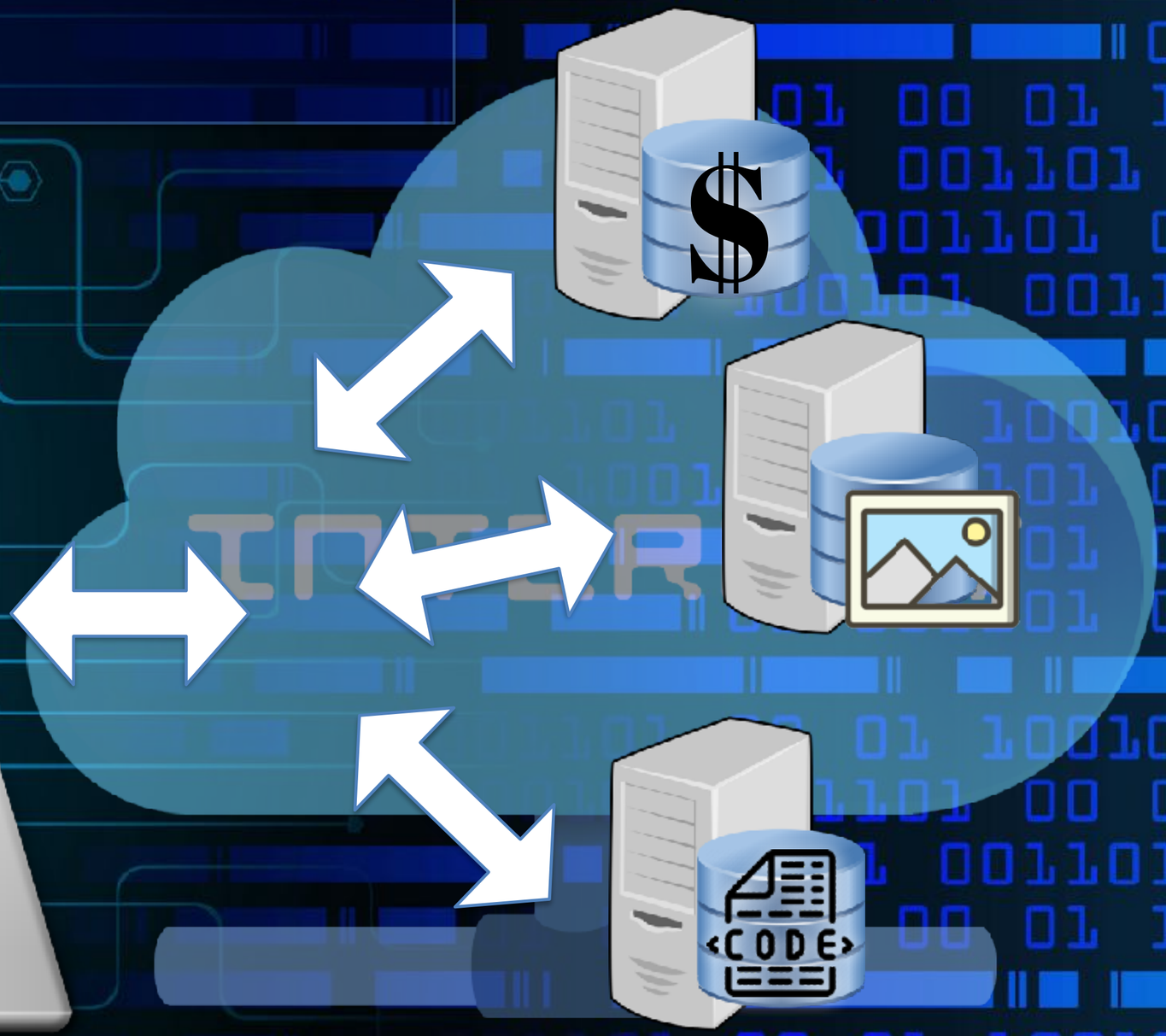

https://onlyfans.com/nice.sp1c3/media
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Search
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
Hide extension URLs
All
Fetch/XHR
JS
CSS
Blocked requests
3rd-party requests
1000 ms
2000 ms
3000 ms
4000 ms
5000 ms
6000 ms
7000 ms
8000 ms
9000 ms
10000 ms
Name
Headers
Payload
Preview
Response
Initiator
Timing
header.jpg
avatar.jpg
data:image/png;base...
300x300_9df31da1d74fb4c9c0729dde2f7...
300x300_a5086952b865d50a8858b683e2...
300x300_ee4138d4c6640b3a641003ff88d...
300x300_5d8ff94bd8123b63a6bf2cdafc6f...
2316x3088_9df
3840x2880_a5
1170x551_5d8f
Open in Sources panel
Open in new tab
Clear browser cache
Clear browser cookies
Copy
Block request URL
Block request domain
Sort By
Header Options
Override headers
Override content
Show all overrides
Copy link address
Copy response
Copy stack trace
Copy as PowerShell
Copy as fetch
Copy as Node.js fetch
Copy as cURL
Copy all as PowerShell
Copy all as fetch


Also: Actual Hax

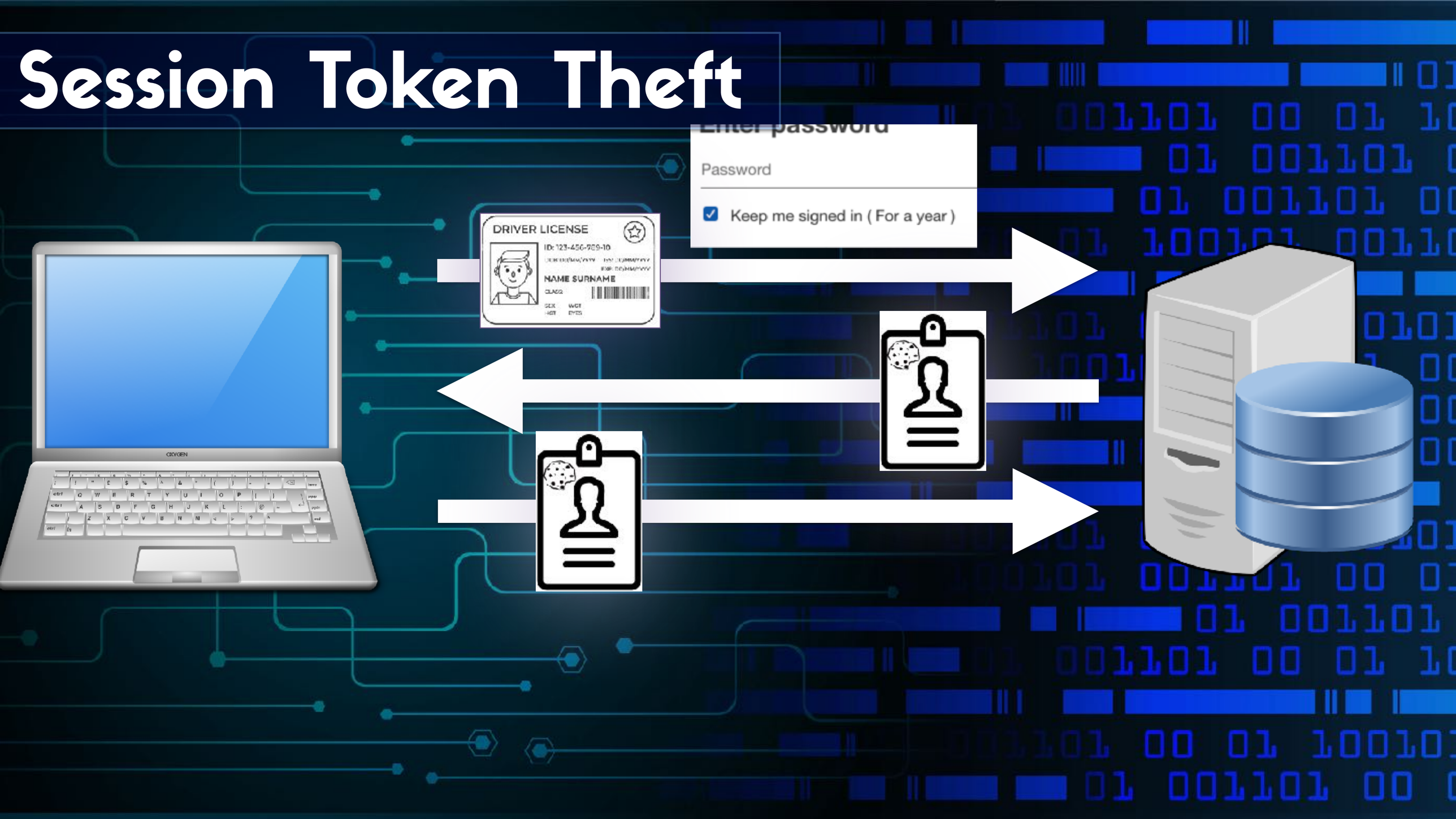
INSECURE APIs

- Most interactive web "sites" are actually applications ("web apps")
- App uses an "Application Programming Interface" to send/ receive info & assets
- Many are way too trusting

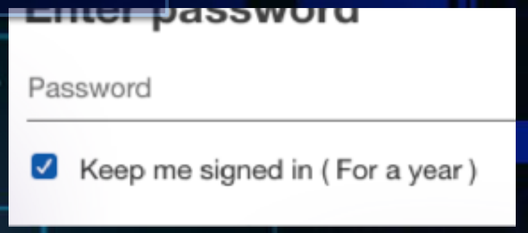
INSECURE APIs

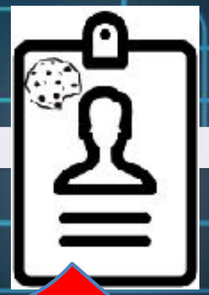


Session Token Theft

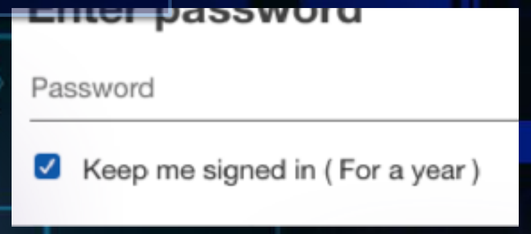


Session Token Theft





Session Token Theft



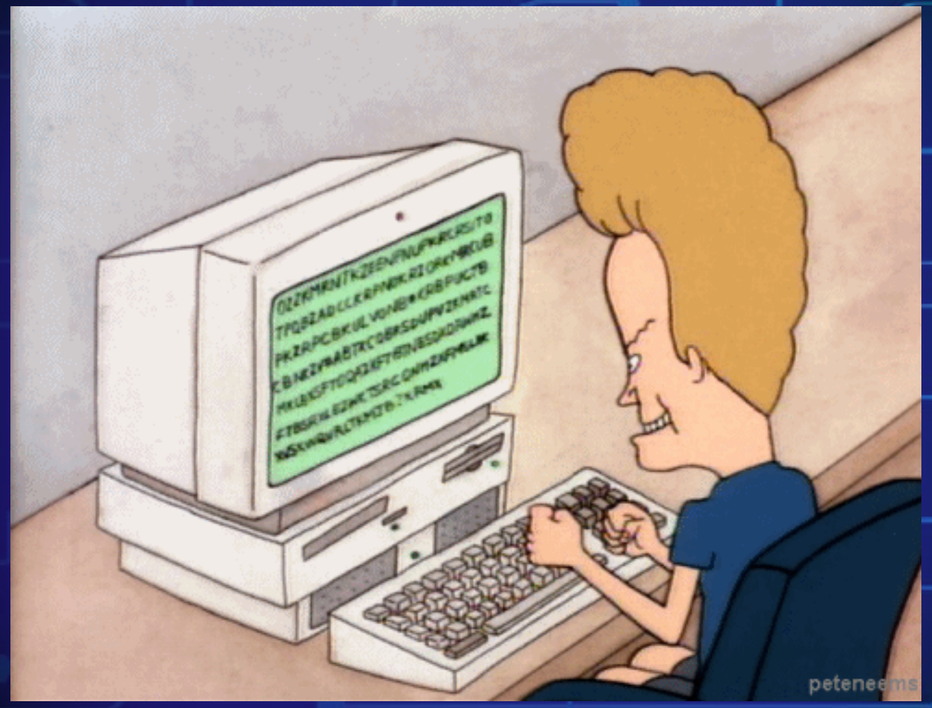
Session Token Theft

- Stolen via browser or directly from the files in your computer
- Most often using malicious links in emails or malicious sites
- Sometimes requires no user interaction (“drive-by” attacks)

Session Token Theft

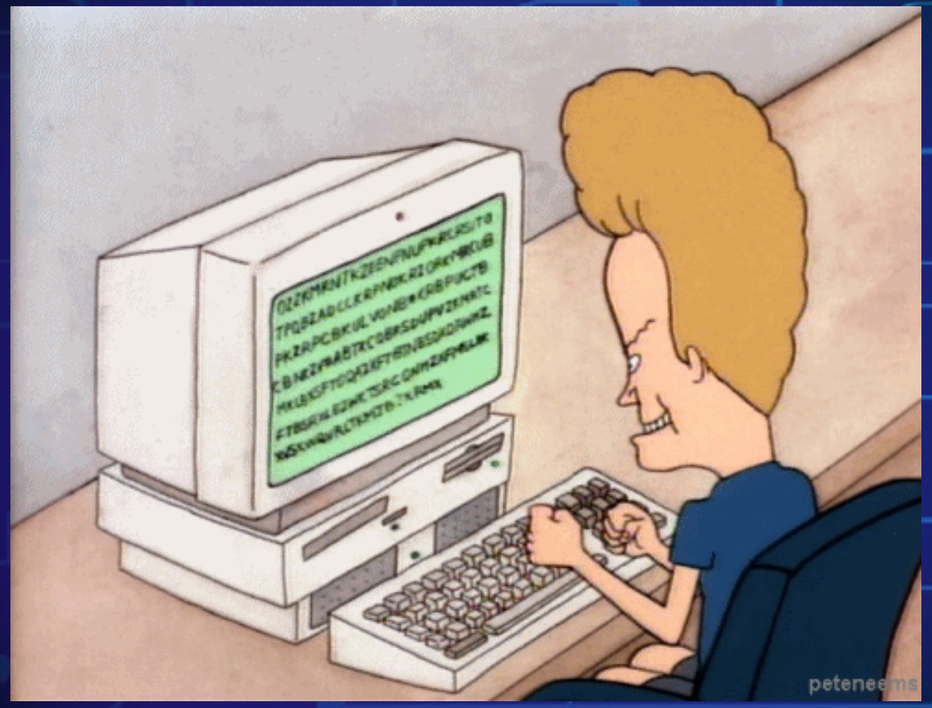
- Stolen via browser or directly from the files in your computer
- Most often using malicious links in emails or malicious sites
- Sometimes requires no user interaction (“drive-by” attacks)

Other Hacks



- RATs (Remote Access Terminal) - Mainly for spying via cams but can enable file access
- Compromised communication apps
- Apps which are fully-functional and useful but cheating on you on the backend

Other Hacks



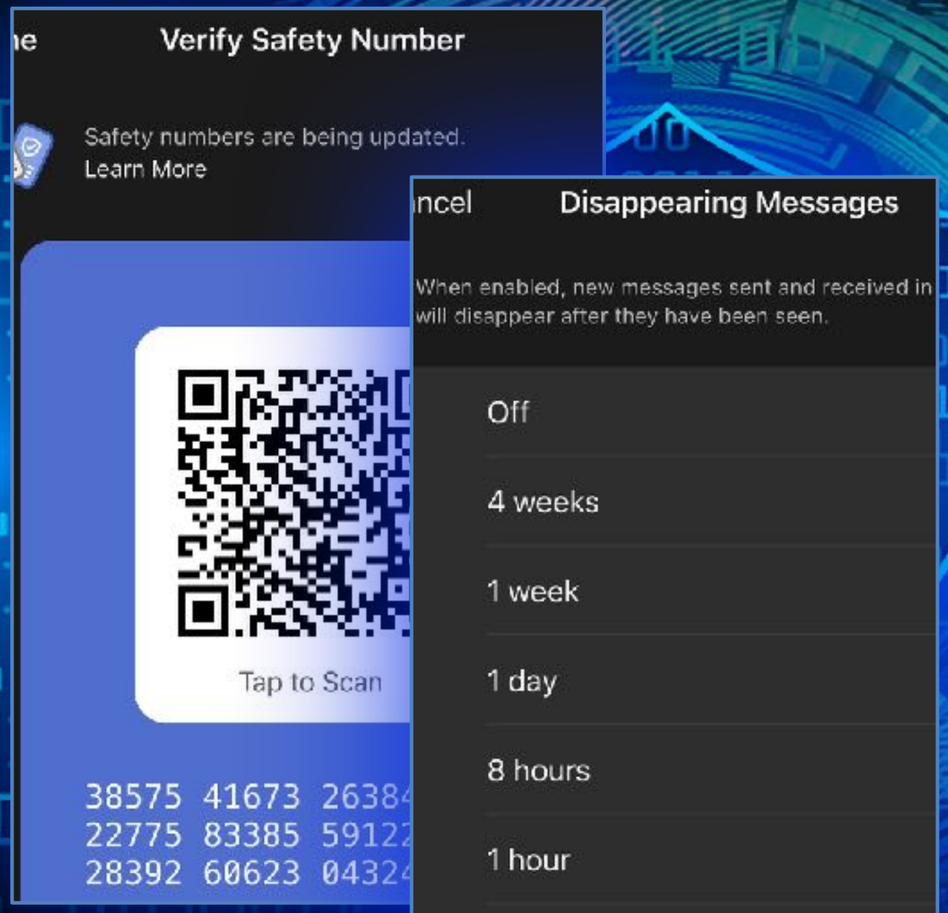
- RATs (Remote Access Terminal) - Mainly for spying via cams but can enable file access
- Compromised communication apps
- Apps which are fully-functional and useful but cheating on you on the backend

MITIGATING CONTROLS

MITIGATING CONTROLS

- Use a *good* password manager
  - Bank & PW Manager PWs should be long, memorized and never digitally documented
  - Use extremely long, complex and unique passwords
  - Enable MFA wherever possible

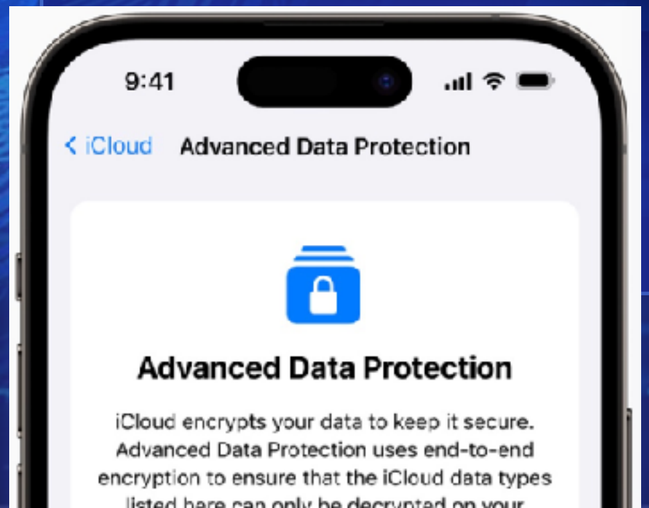
MITIGATING CONTROLS



- Operate with a conscious understanding that digital privacy is nonexistent
- Do not store or transmit anything private using systems you do not control
  - Use comms with E2E encryption
  - Verify the recipient & set short message expiration times

MITIGATING CONTROLS

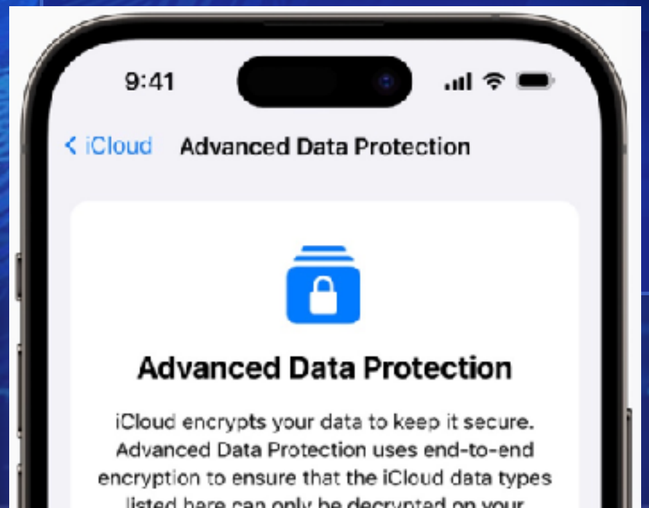
- Obscure your face \ ID features
  - Can still be fun! Extreme makeup, masks, or Snap Lenses
- "Zero Knowledge" Data Backups



SPIDEROAK

MITIGATING CONTROLS

- Obscure your face \ ID features
  - Can still be fun! Extreme makeup, masks, or Snap Lenses
- "Zero Knowledge" Data Backups



SPIDEROAK

SAVING RYAN'S PRIVATES

Johnny Xmas, CISSP, GIAC
Technical Director of Training, GRIMM
https://grimm.rip