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
- Troublemaker
- Educator
- Community Leader
- **HACKER**


STATS!

STATS!

STATS!

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

It’s impossible to accurately
track this, anyway.

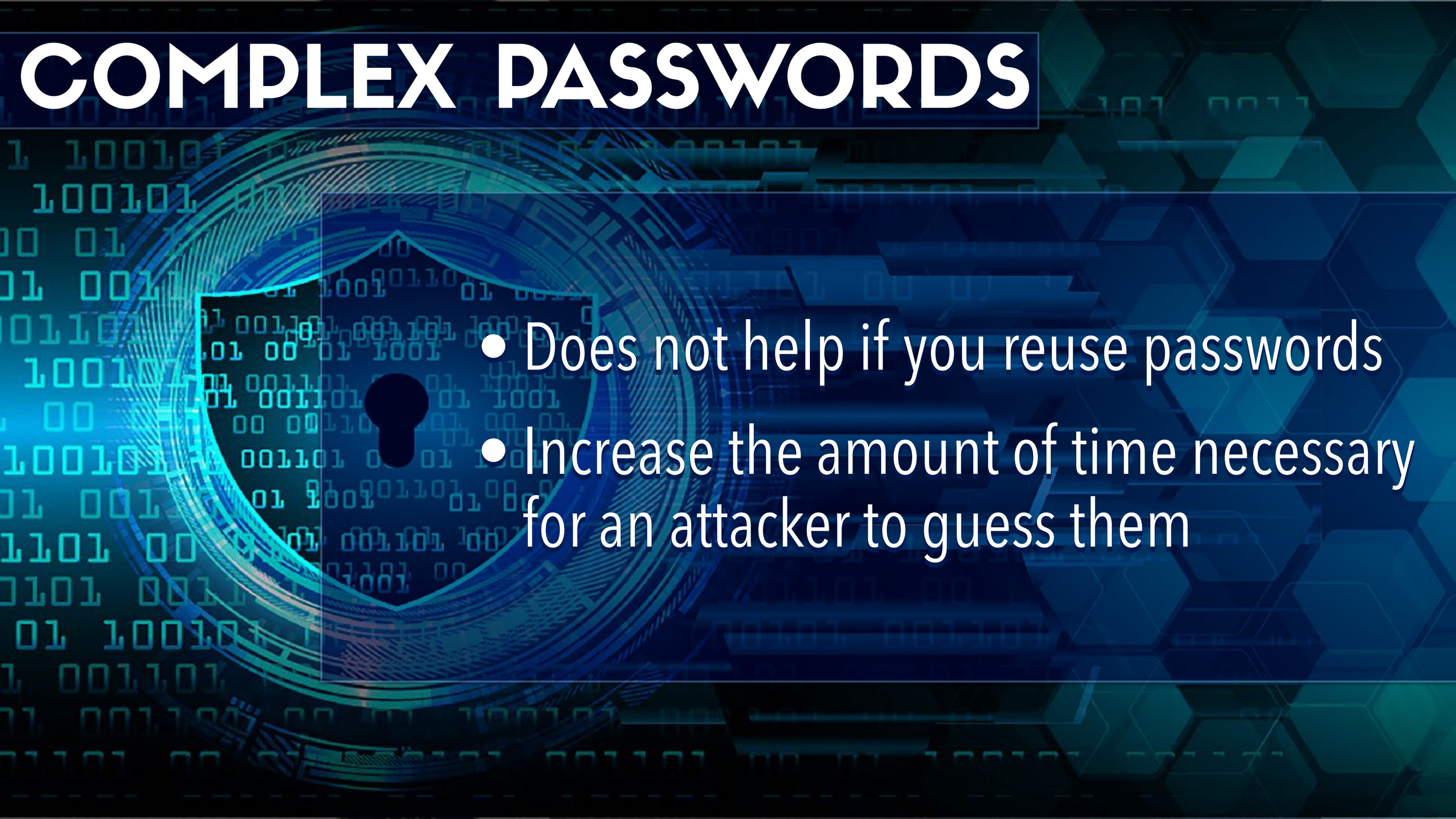
**WE ALL KNOW THIS IS
A HUGE PROBLEM, REGARDLESS**

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



- Does not help if you reuse passwords
- Increase the amount of time necessary for an attacker to guess them

Multi-Factor Auth.

- Like having 2 passwords, one of which rotates
- Great even when your password sucks
- Requires attacker to access the device or service that has your "token"


So How do Leaks Happen, Then?

YOUR PARTNER SUCKS

(In the bad way)

- Intentional Leaks
- Their cybersecurity posture sucks
- They're using a non-encrypting messaging system
  - No End-to-End Encryption
  - No Message Expiration

YOUR PARTNER SUCKS

(In the bad way)

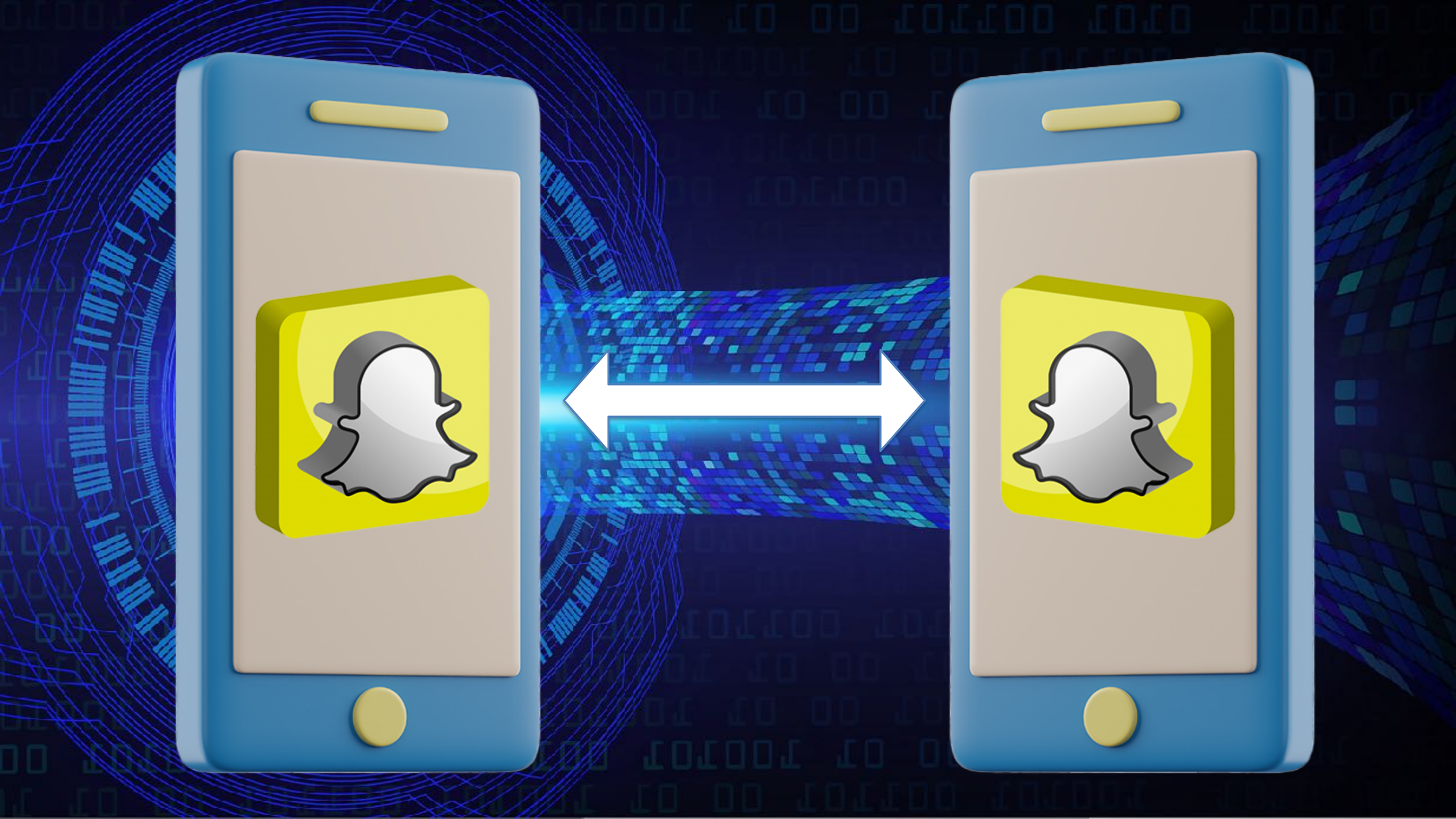
- Intentional Leaks
- Their cybersecurity posture sucks
- They're using a non-encrypting messaging system

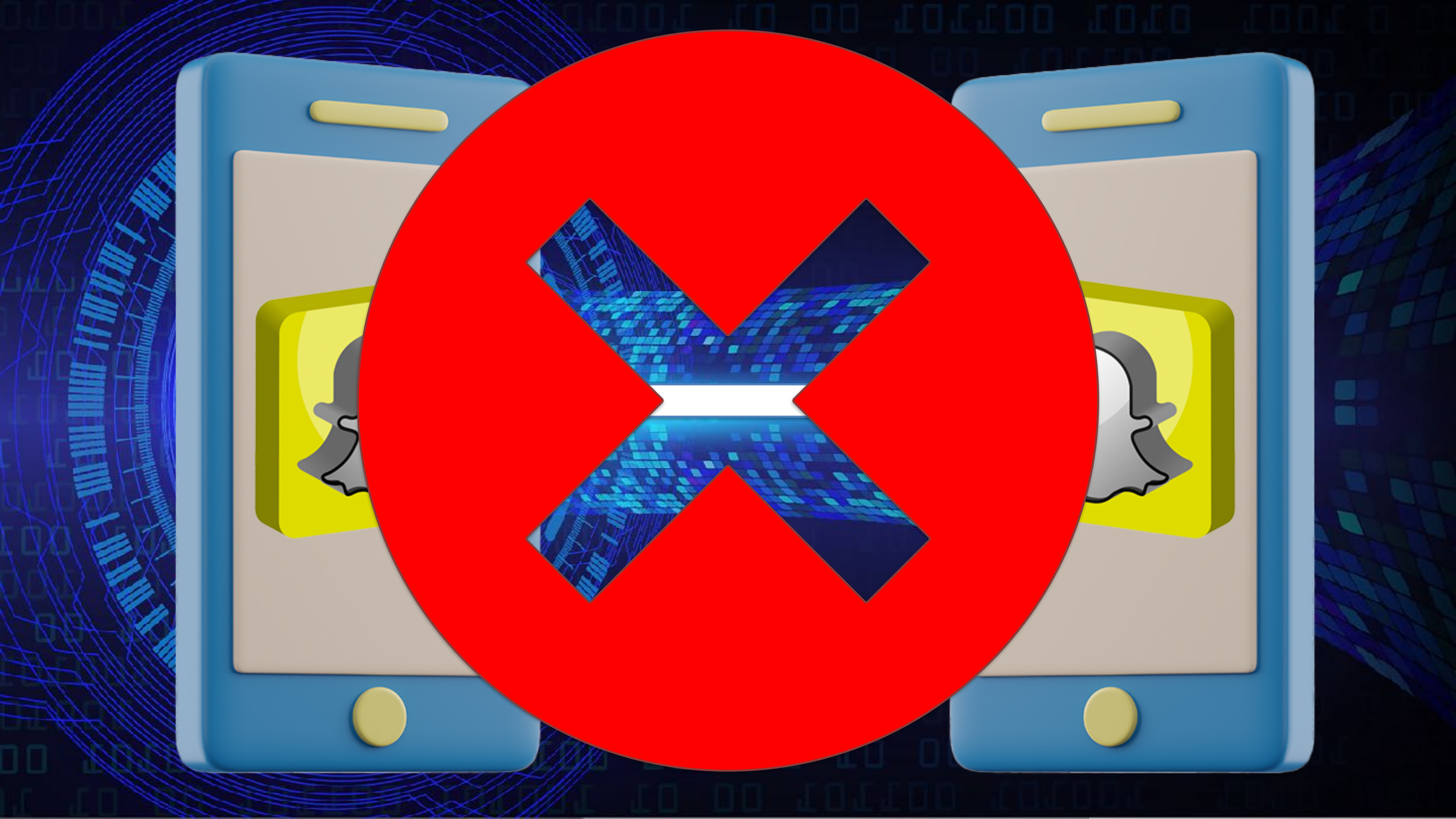
IT IS IMPOSSIBLE FOR ANY GROUP CHAT TO HAVE E2E ENCRYPTION.

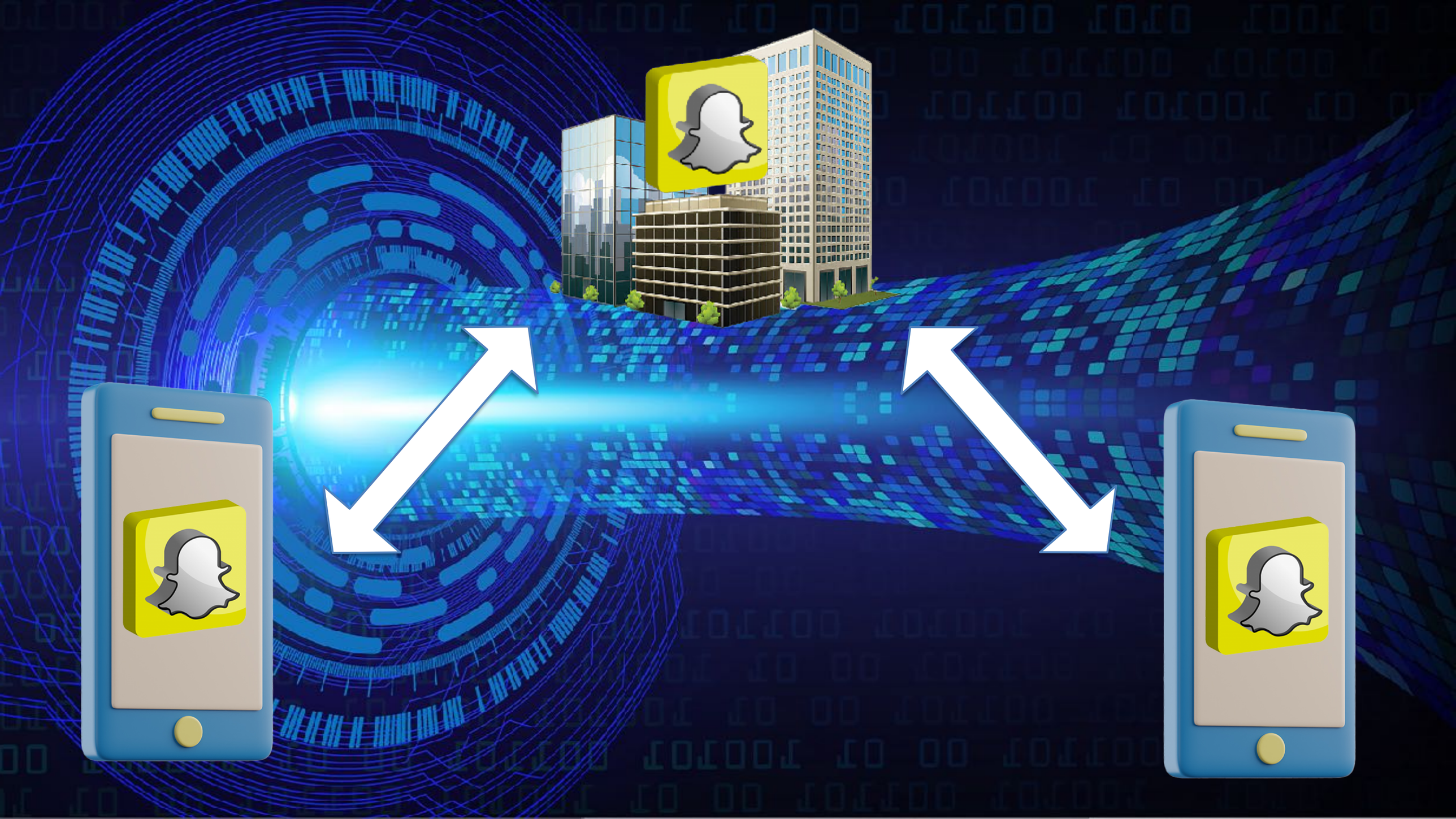
- No End-to-End Encryption
- No Message Expiration

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

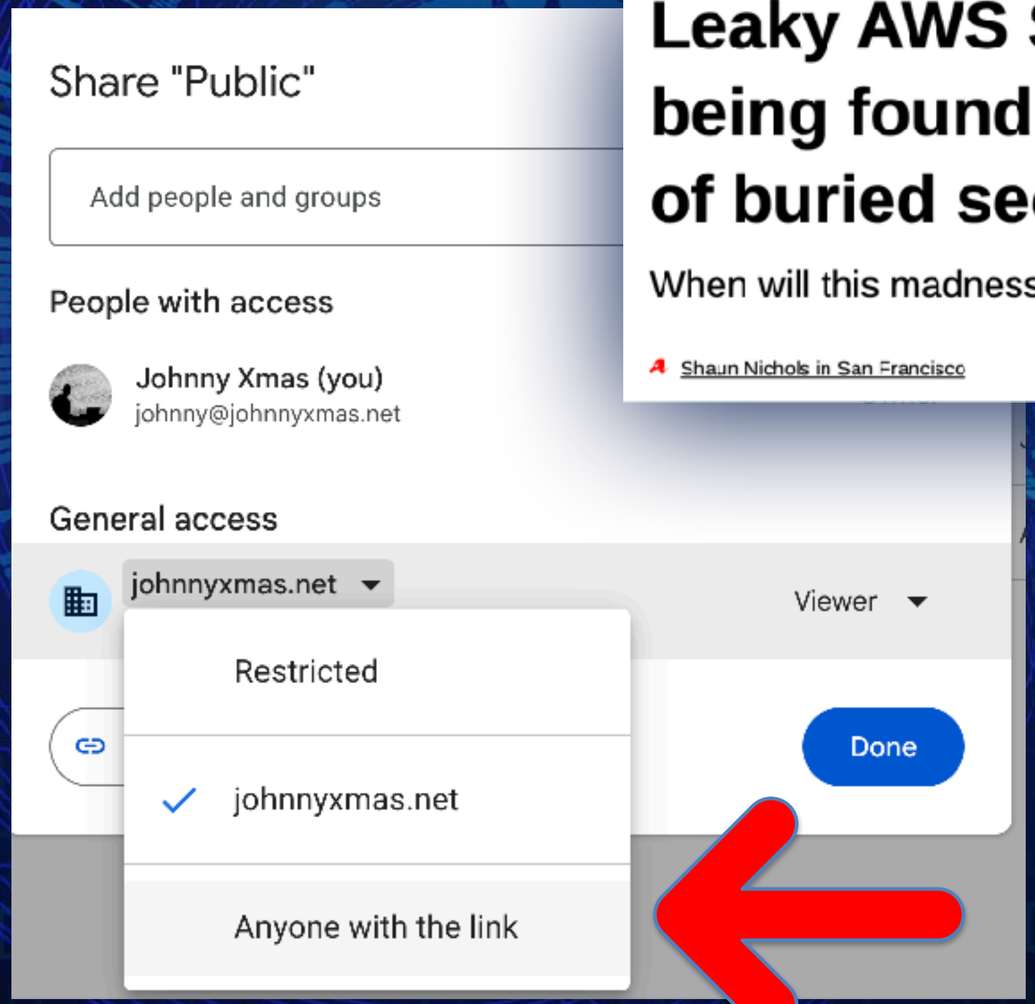
Two former employees said multiple Snap employees abused their access to Snapchat user data several years ago. Those sources, as well as an additional two former employees, a current employee, and a cache of internal company emails obtained by Motherboard, described internal tools that allowed Snap employees 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."

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

You're Using Somebody Else's Computer



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

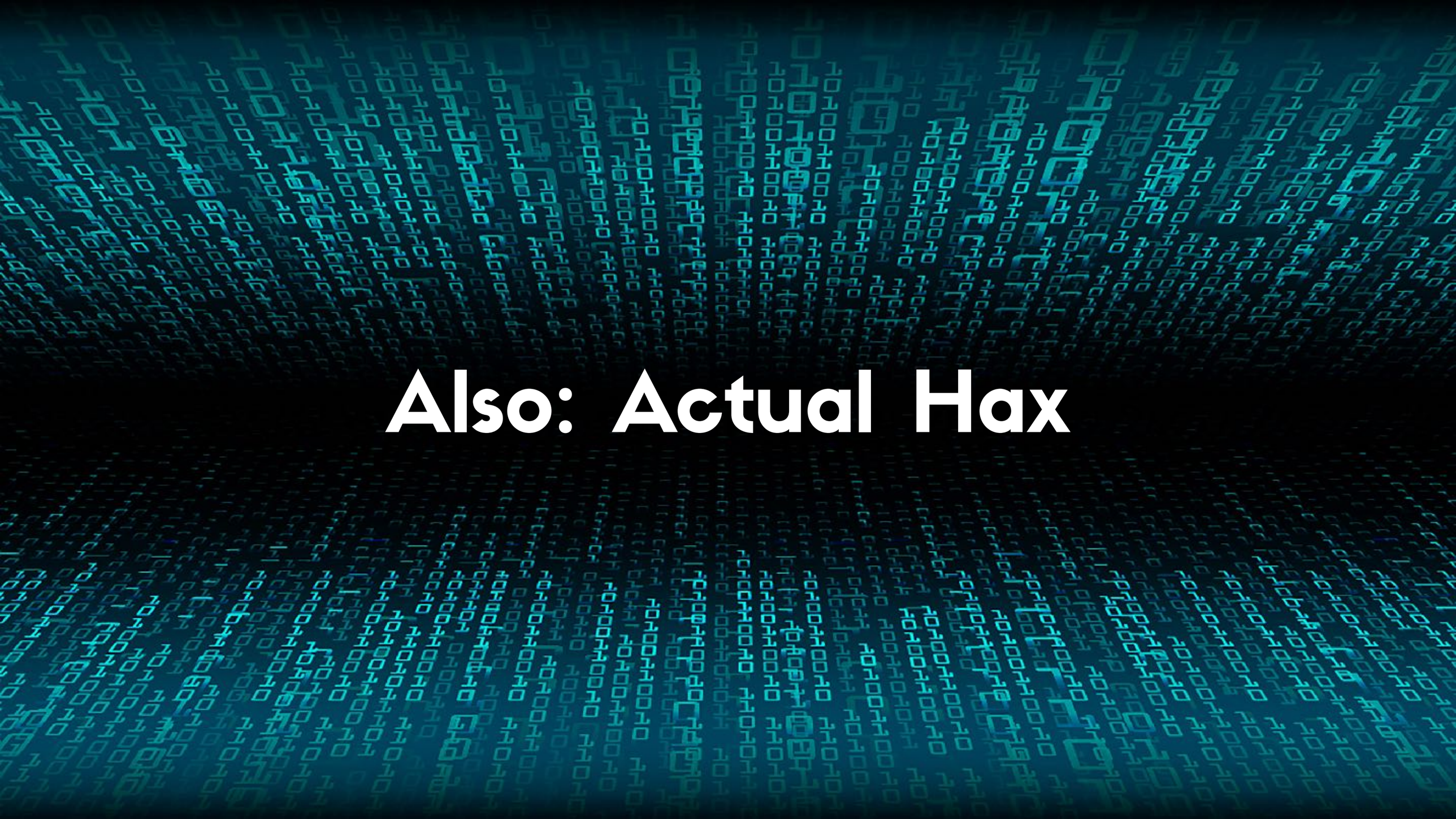
Discord recently fixed this problem…

OnlyFans has it *RIGHT NOW.*

You're Using Somebody Else's Computer

Discord recently fixed this problem…

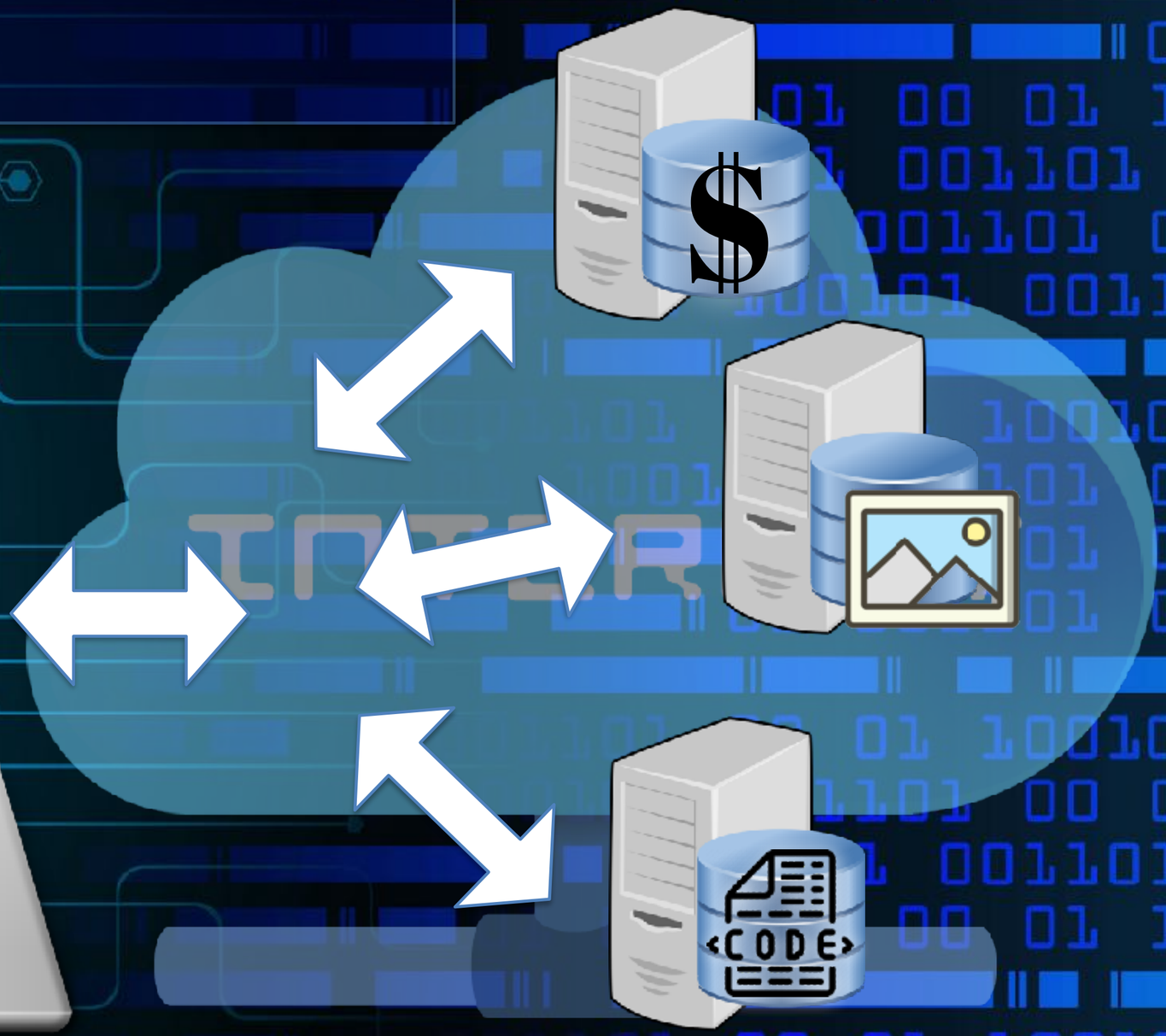
OnlyFans has it *RIGHT NOW.*


Also: Actual Hax

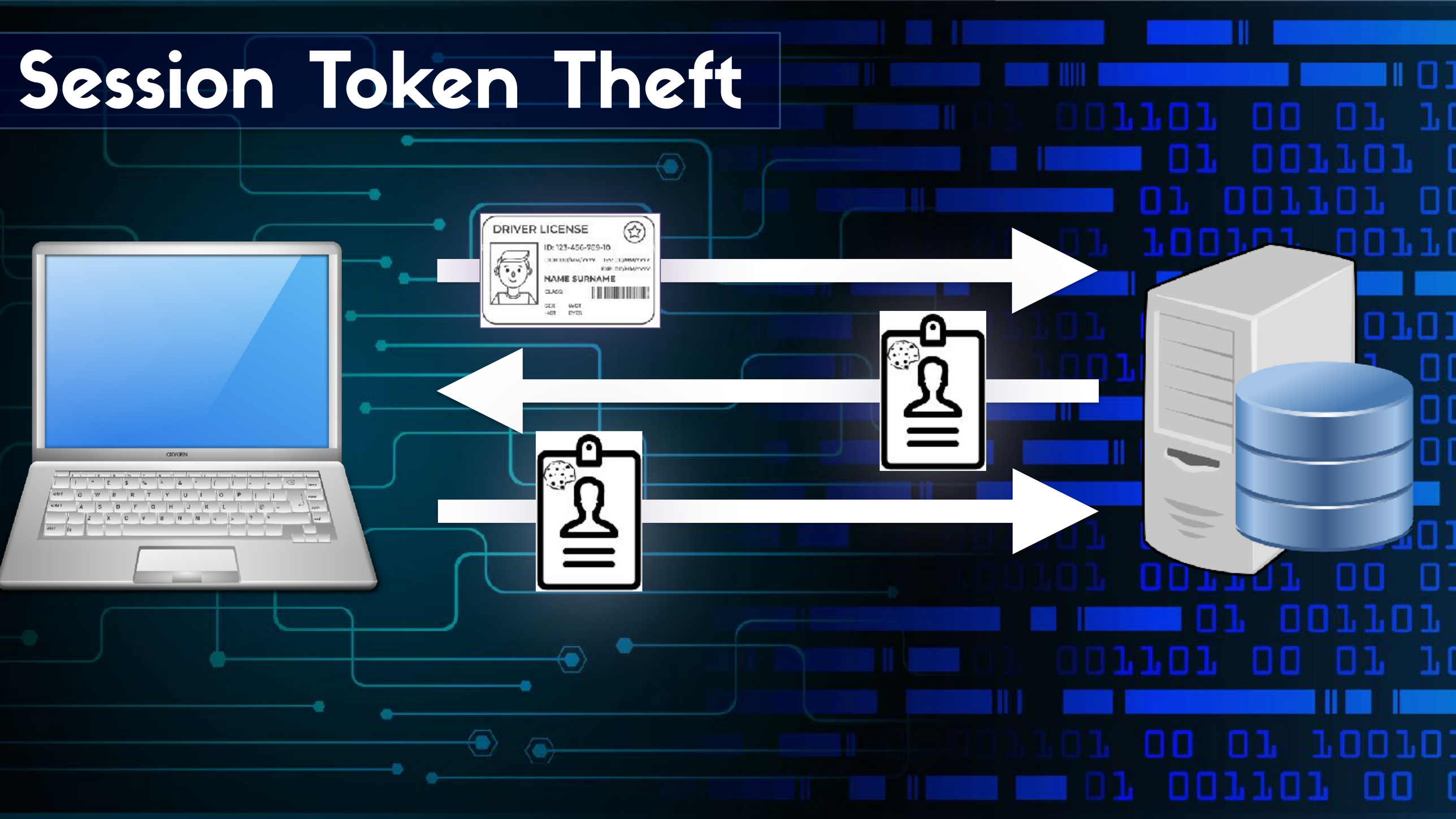
INSECURE APIs

- Most interactive web “sites” are actually applications (“web apps”)
- App uses an “API” pathway and language to send/receive info & assets
- Many are way too trusting

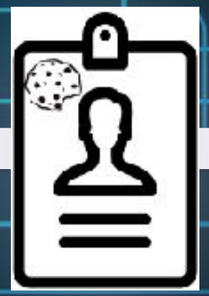
INSECURE APIs



Session Token Theft



Session Token Theft



Session Token Theft

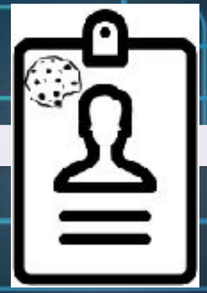
How hackers took over Linus Tech Tips

/ The hackers were able to take over three Linus Media Group YouTube channels by targeting session tokens.

By Jay Peters, a news editor who writes about technology, video games, and virtual worlds. He's submitted several accepted emoji proposals to the Unicode Consortium.

Mar 24, 2023, 12:25 PM EDT | 49 Comments / 49 New

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.



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

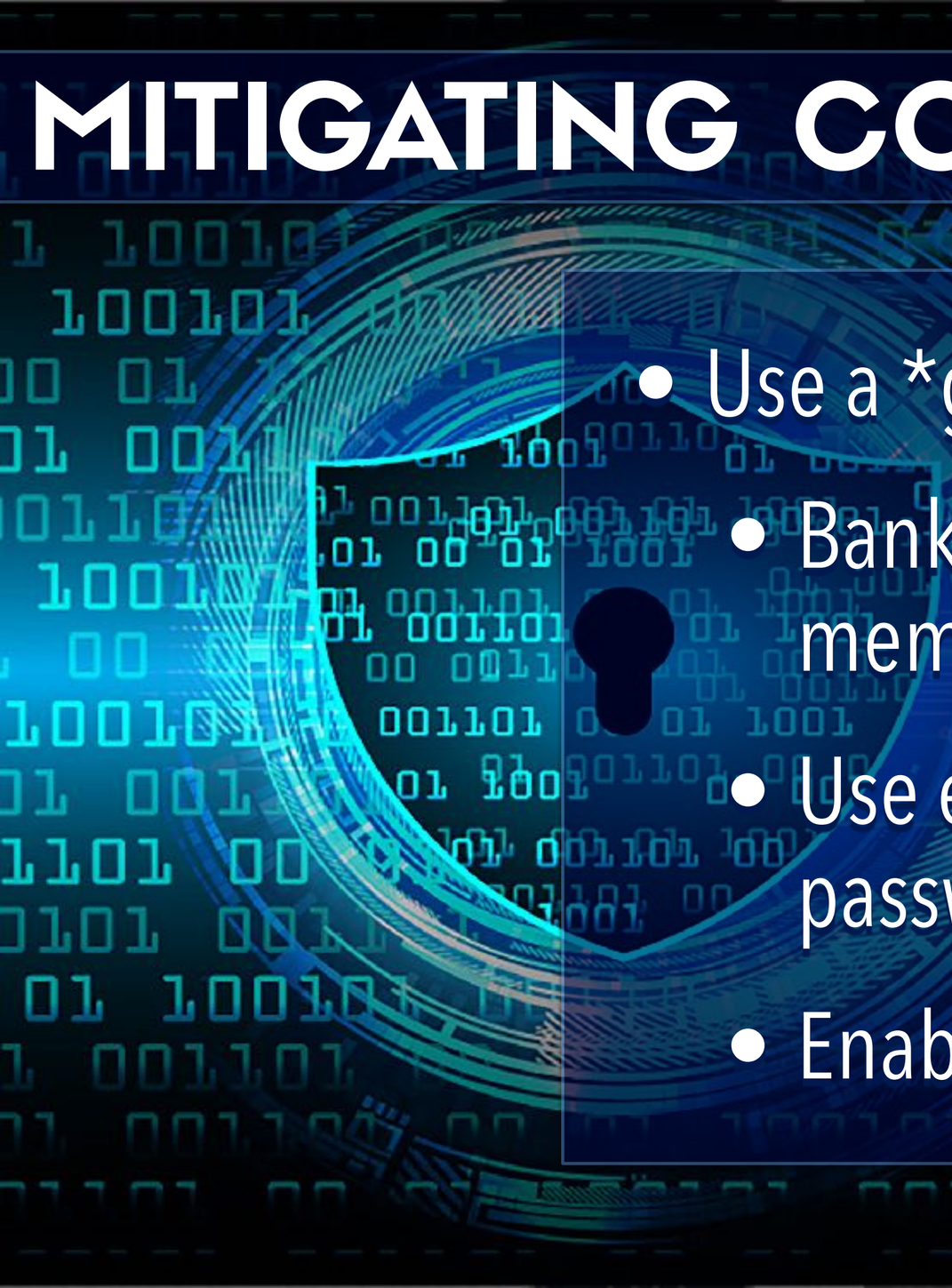
- Stolen via browser or directly from the files in your computer
- Most often using malicious links in emails or malicious sites
- Sometimes requires no user interaction (“drive-by” attacks)

Other Hacks

- RATs (Remote Access Terminal) - Mainly for spying via webcams / security cams but can enable file access
- Compromised communication (or other) apps
  - Encryption doesn't matter if they grab the message before it's encrypted

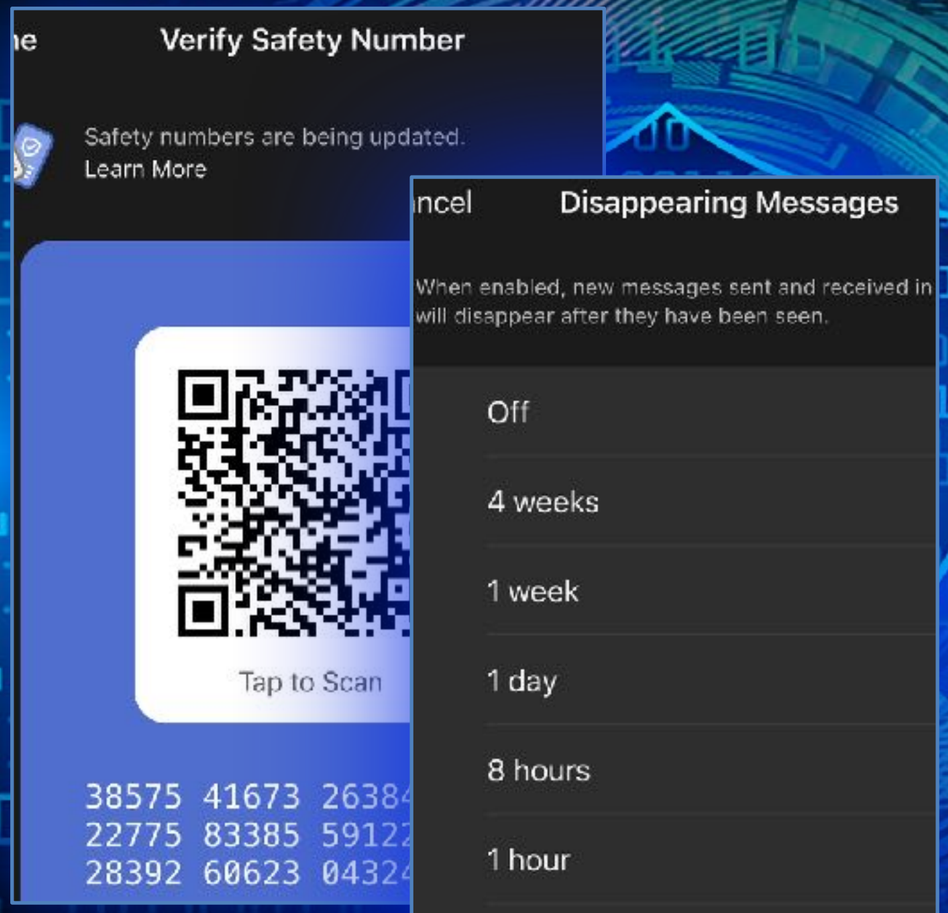
MITIGATING CONTROLS

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
  - Use comms with E2E encryption
    - Verify the recipient & set short message expiration times
- Do not store or transmit anything private using systems you do not control

SAVING RYAN'S PRIVATES

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