Security Vulnerabilities within a PSAP

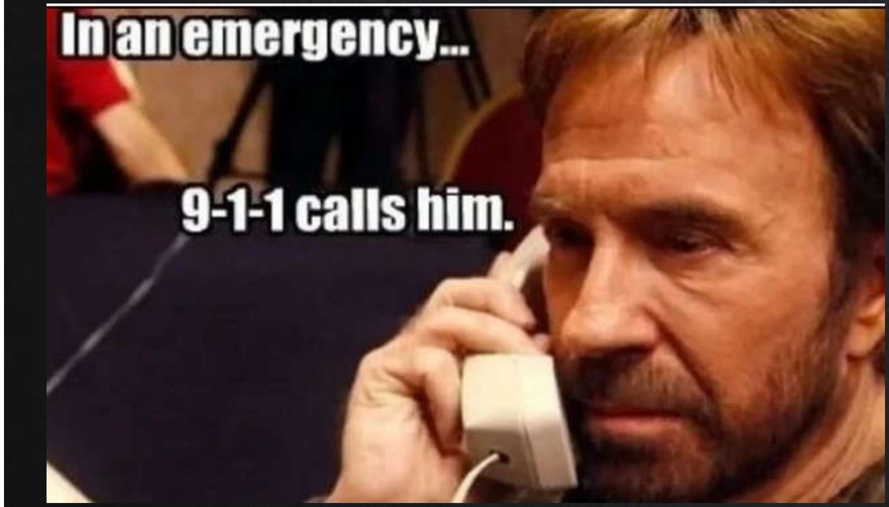
Friend: I bet you guys have like super high tech systems and stuff for something as important as 911

Dispatch centers:

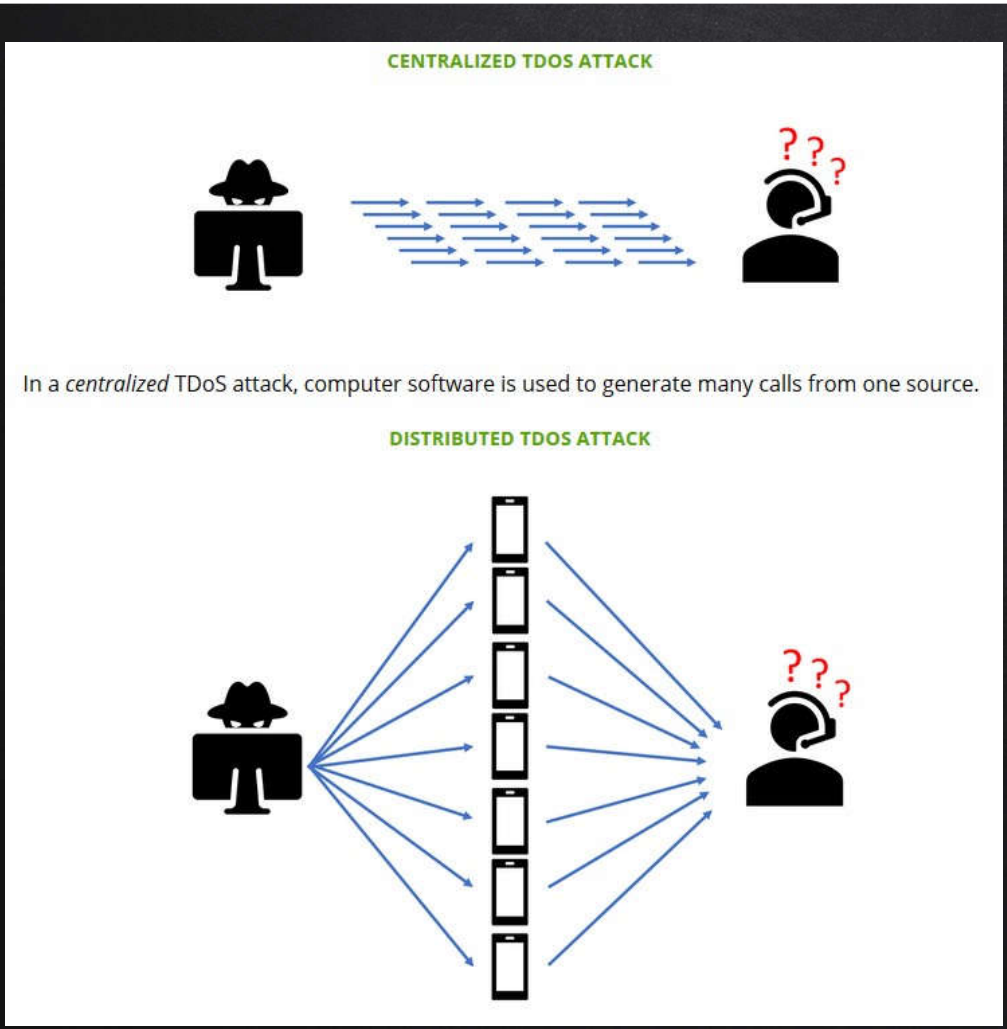
Christine Giglio

CAD Administrator
Bedford County Emergency Communications
Bedford County, VA

TOPICS



- Telephone Denial of Service Attacks
- Threats to Network/Systems
- Threats to Citizens and First Responders
- Personal Tale of Ransomware Woes and the Lessons Learned.



CENTRALIZED TDOS ATTACK

In a *centralized* TDoS attack, computer software is used to generate many calls from one source.

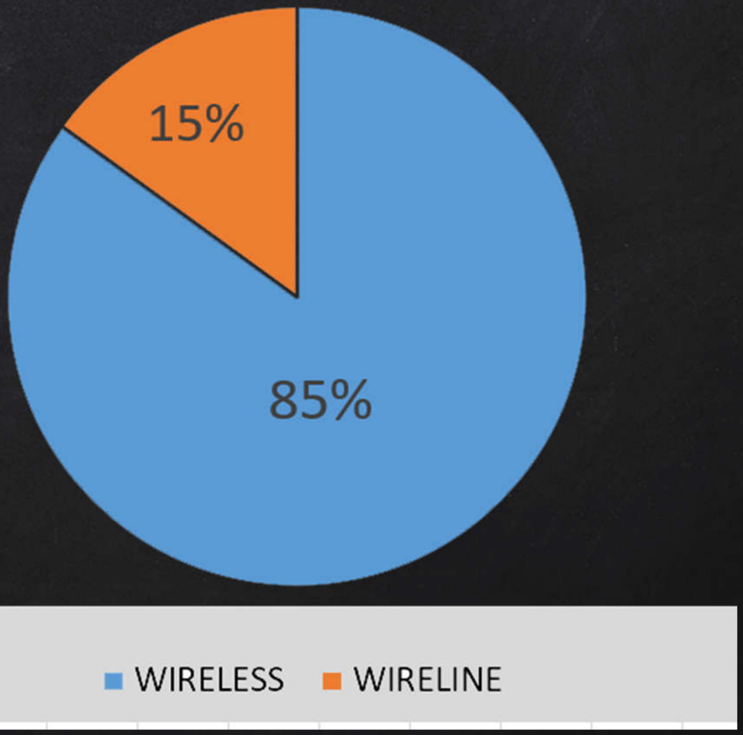
DISTRIBUTED TDOS ATTACK

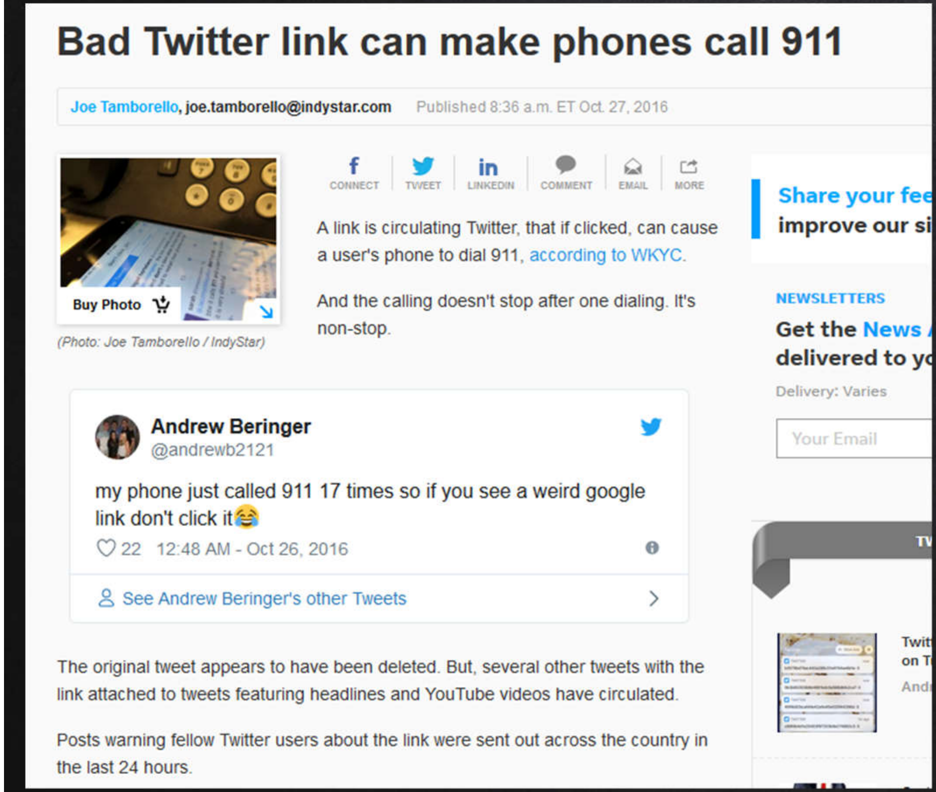
TELEPHONY DENIAL OF SERVICE

TDoS

Image from https://transnexus.com/tdos-prevention/

TDoS
911 LINES





Bad Twitter link can make phones call 911

Joe Tamborello, joe.tamborello@indystar.com Published 8:36 a.m. ET Oct. 27, 2016

(Photo: Joe Tamborello / IndyStar)

A link is circulating Twitter, that if clicked, can cause a user's phone to dial 911, according to WKYC.

And the calling doesn't stop after one dialing. It's non-stop.

Andrew Beringer
@andrewb2121

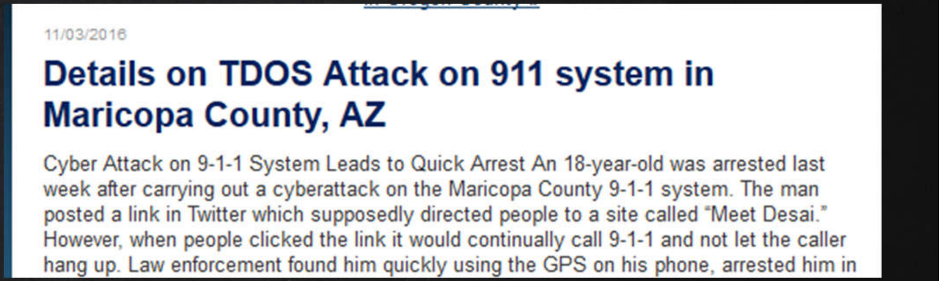
my phone just called 911 17 times so if you see a weird google link don't click it😂

♡ 22 12:48 AM - Oct 26, 2016

See Andrew Beringer's other Tweets

The original tweet appears to have been deleted. But, several other tweets with the link attached to tweets featuring headlines and YouTube videos have circulated.

Posts warning fellow Twitter users about the link were sent out across the country in the last 24 hours.



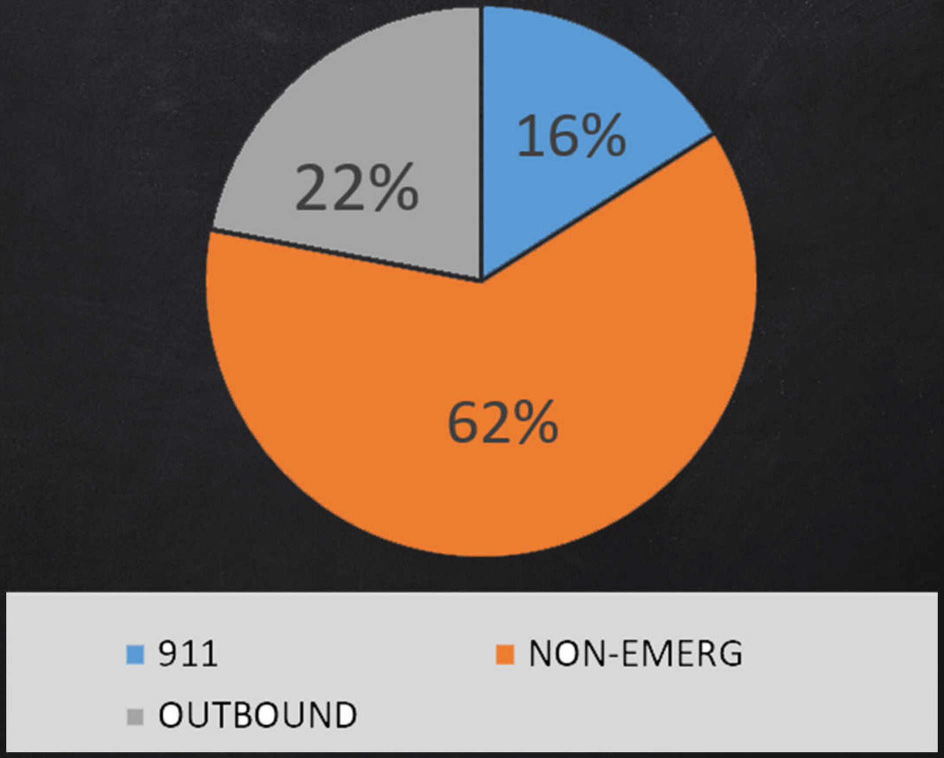
11/03/2016

Details on TDOS Attack on 911 system in Maricopa County, AZ

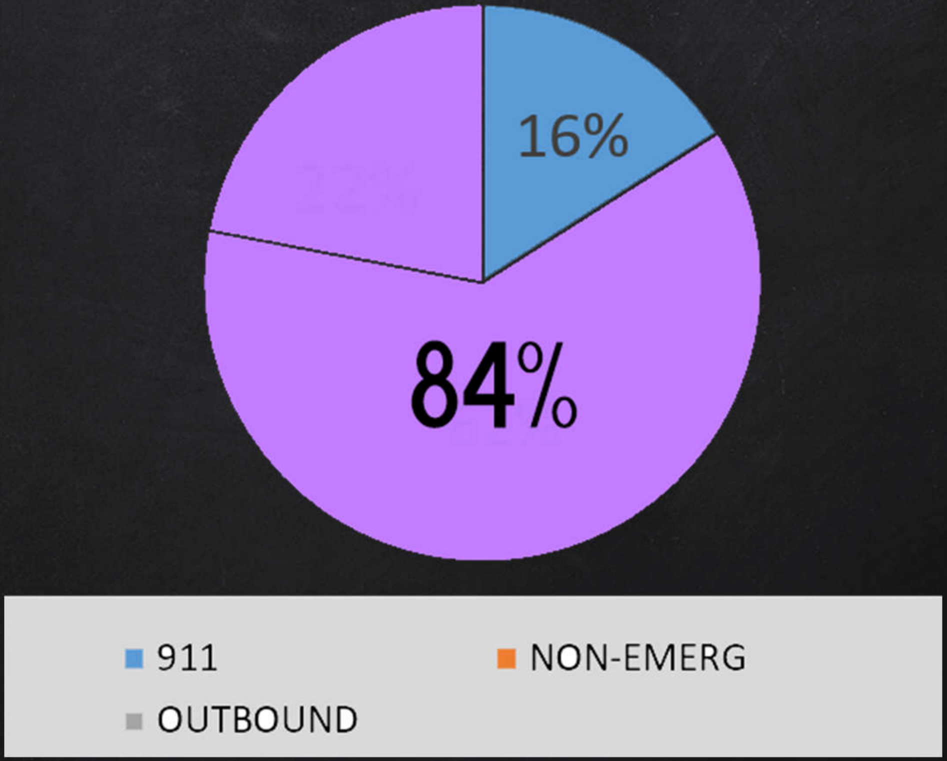
Cyber Attack on 9-1-1 System Leads to Quick Arrest An 18-year-old was arrested last week after carrying out a cyberattack on the Maricopa County 9-1-1 system. The man posted a link in Twitter which supposedly directed people to a site called "Meet Desai." However, when people clicked the link it would continually call 9-1-1 and not let the caller hang up. Law enforcement found him quickly using the GPS on his phone, arrested him in

TDoS

NON-EMERGENCY LINES



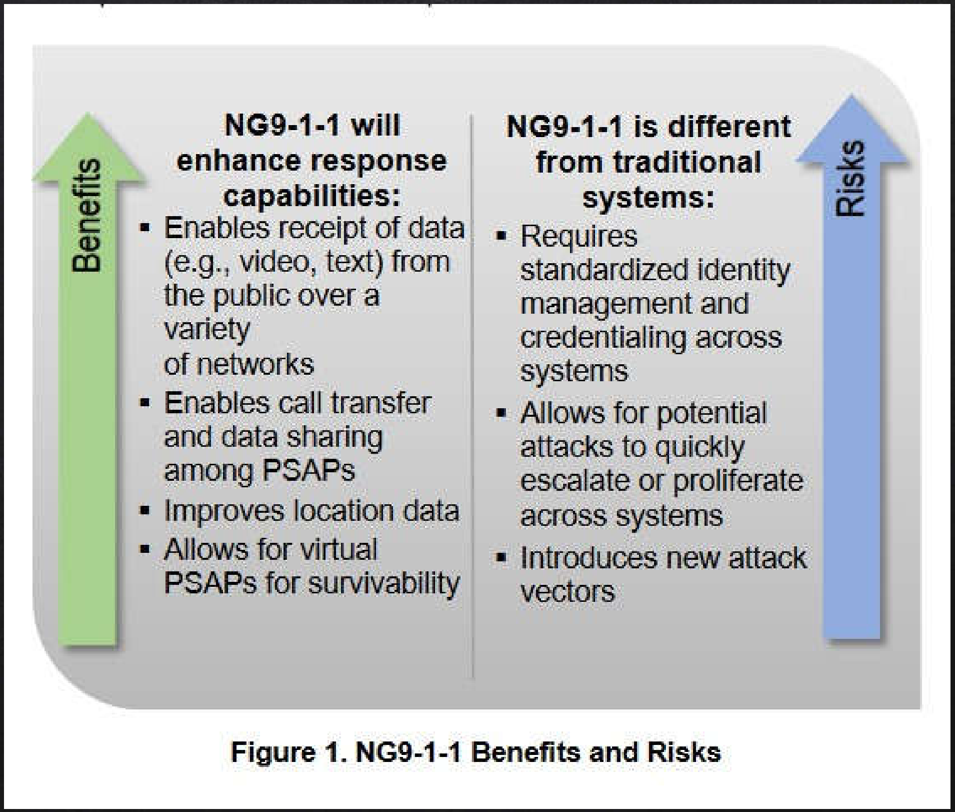
TDoS
NON-EMERGENCY LINES



TDoS

NEXTGEN 911

Image from CISA Cyber Risks to Next Generation 9-1-1 White Paper 2019



NG9-1-1 will enhance response capabilities:

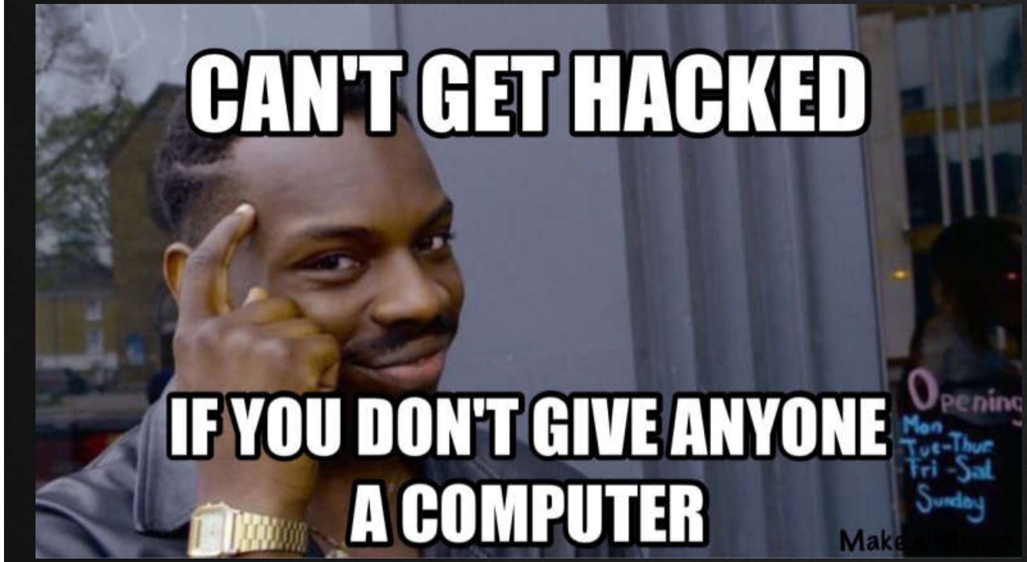
- Enables receipt of data (e.g., video, text) from the public over a variety of networks
- Enables call transfer and data sharing among PSAPs
- Improves location data
- Allows for virtual PSAPs for survivability

NG9-1-1 is different from traditional systems:

- Requires standardized identity management and credentialing across systems
- Allows for potential attacks to quickly escalate or proliferate across systems
- Introduces new attack vectors

Figure 1. NG9-1-1 Benefits and Risks

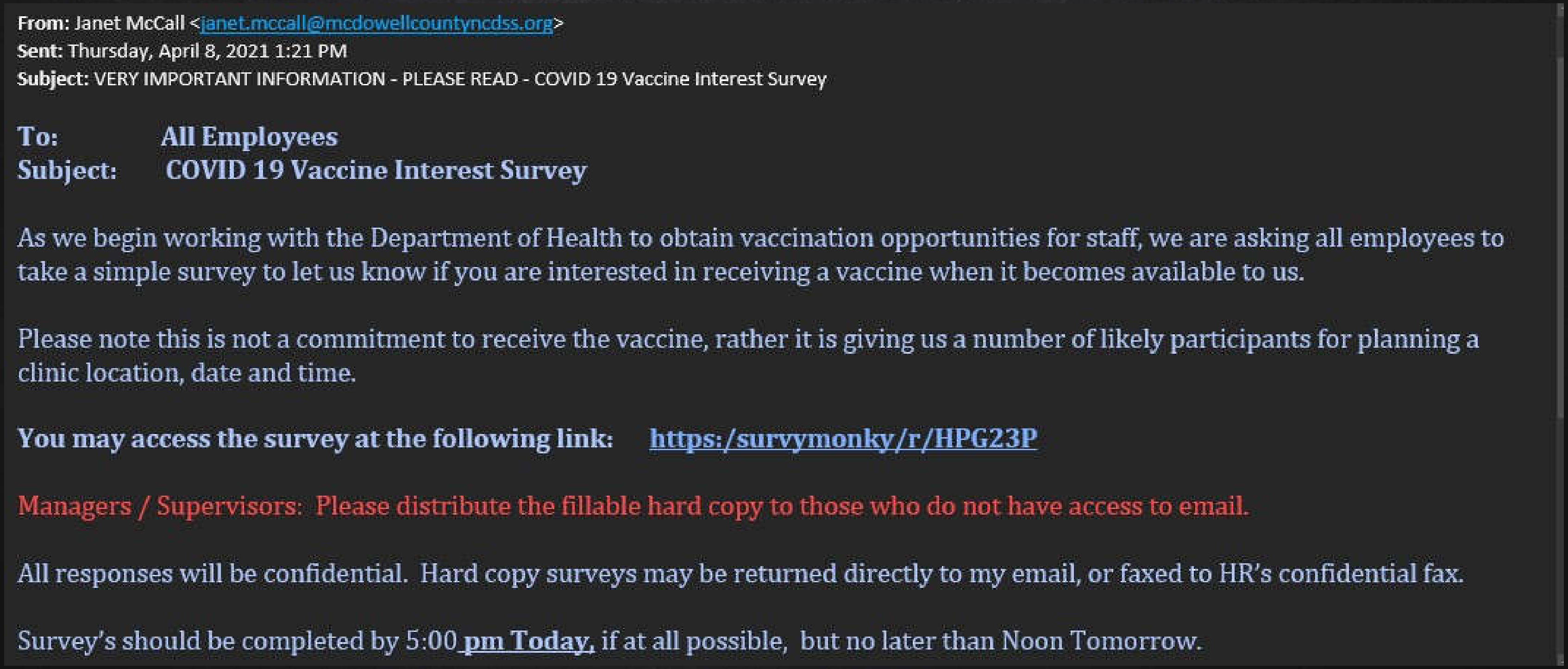
OTHER THREATS



- Any system with Internet access
- System Vulnerability (anything on cve.mitre.org)
- E-mail: Attachment
- E-mail: Phishing link
- Hoax calls/Swatting and Freedom of Information Act

E-MAILS

PHISHING OR ATTACHMENT BASED



From: Janet McCall <janet.mccall@mcdowellcountyncdss.org>
Sent: Thursday, April 8, 2021 1:21 PM
Subject: VERY IMPORTANT INFORMATION - PLEASE READ - COVID 19 Vaccine Interest Survey

To: **All Employees**
Subject: **COVID 19 Vaccine Interest Survey**

As we begin working with the Department of Health to obtain vaccination opportunities for staff, we are asking all employees to take a simple survey to let us know if you are interested in receiving a vaccine when it becomes available to us.

Please note this is not a commitment to receive the vaccine, rather it is giving us a number of likely participants for planning a clinic location, date and time.

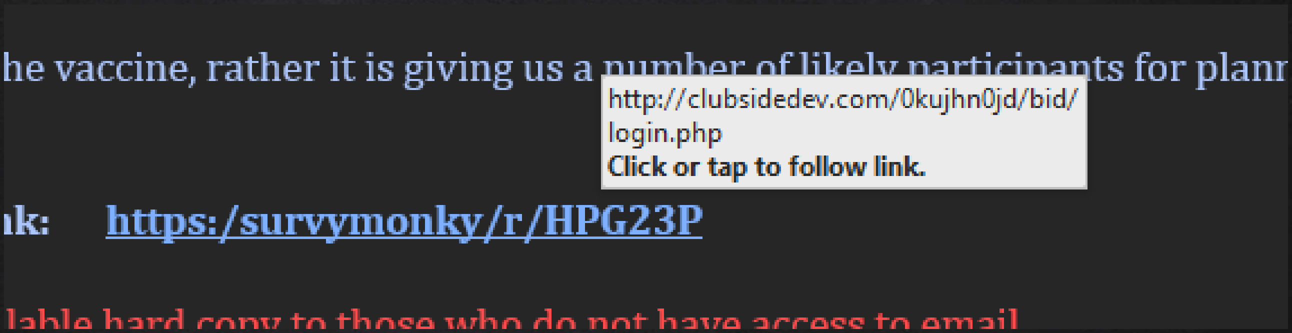
You may access the survey at the following link: **https:/survymonky/r/HPG23P**

Managers / Supervisors: Please distribute the fillable hard copy to those who do not have access to email.

All responses will be confidential. Hard copy surveys may be returned directly to my email, or faxed to HR's confidential fax.

Survey's should be completed by 5:00 **pm Today,** if at all possible, but no later than Noon Tomorrow.

HOVER OVER LINK IN E-MAIL TO SHOW ACTUAL ADDRESS



he vaccine, rather it is giving us a number of likely participants for plann

http://clubsidedev.com/0kujhn0jd/bid/login.php
Click or tap to follow link.

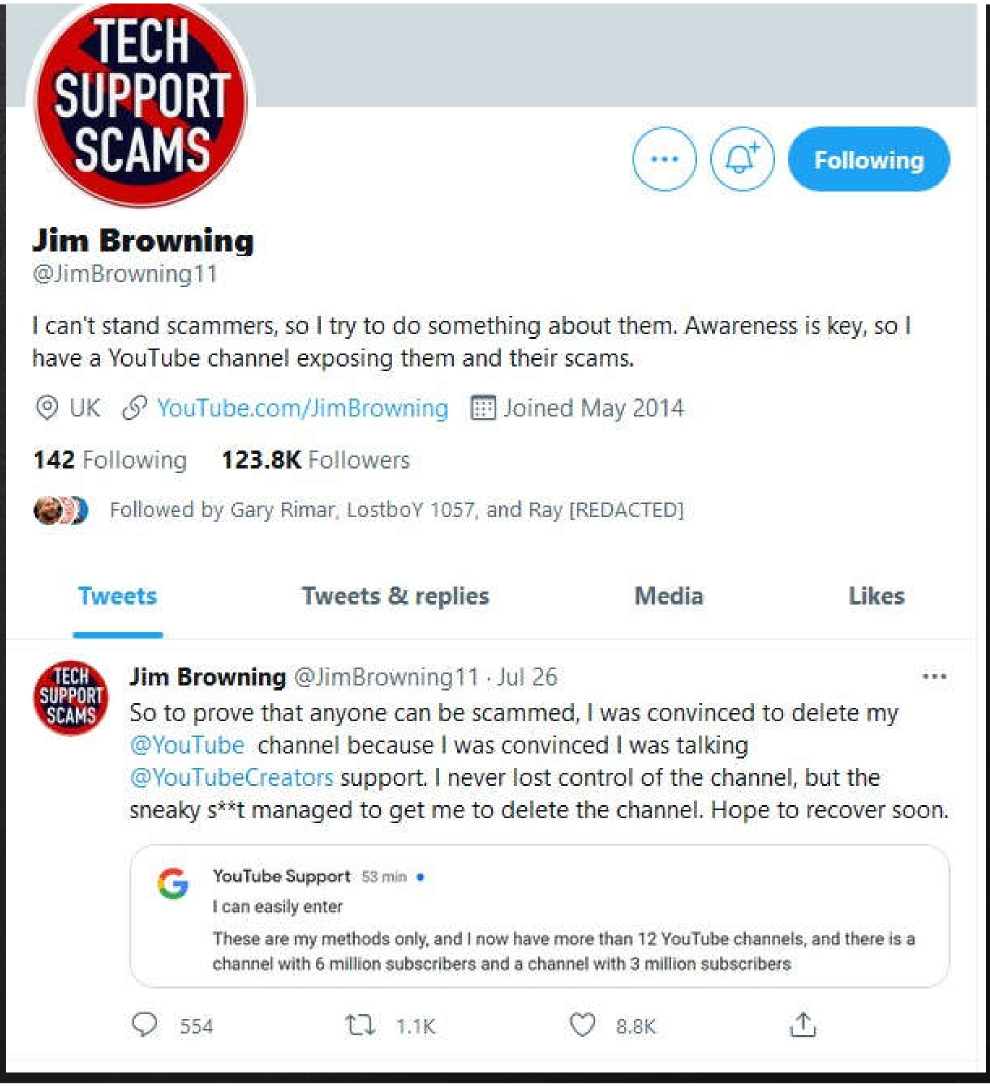
ık: **https:/survymonky/r/HPG23P**

lable hard copy to those who do not have access to email

IN THE WILD!

THINK YOU WON'T CLICK?

ANYONE CAN GET HIT!



Jim Browning
@JimBrowning11

I can't stand scammers, so I try to do something about them. Awareness is key, so I have a YouTube channel exposing them and their scams.

UK YouTube.com/JimBrowning Joined May 2014

142 Following **123.8K** Followers

Followed by Gary Rimar, LostboY 1057, and Ray [REDACTED]

Jim Browning @JimBrowning11 · Jul 26

So to prove that anyone can be scammed, I was convinced to delete my @YouTube channel because I was convinced I was talking @YouTubeCreators support. I never lost control of the channel, but the sneaky s**t managed to get me to delete the channel. Hope to recover soon.

YouTube Support 53 min

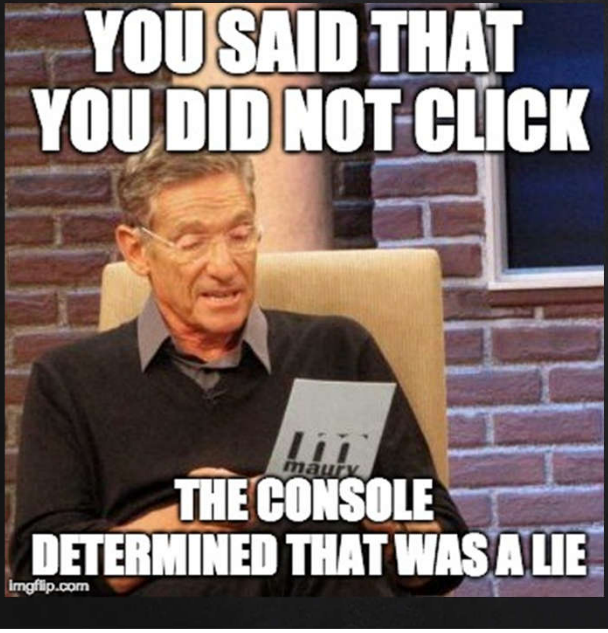
I can easily enter

These are my methods only, and I now have more than 12 YouTube channels, and there is a channel with 6 million subscribers and a channel with 3 million subscribers

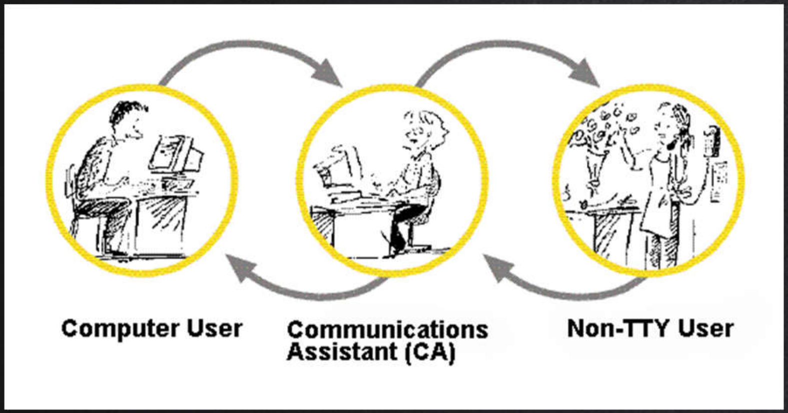
EDUCATION, EDUCATION, EDUCATION

Security Awareness Computer-Based Training

Check your info on:
https://haveibeenpwned.com



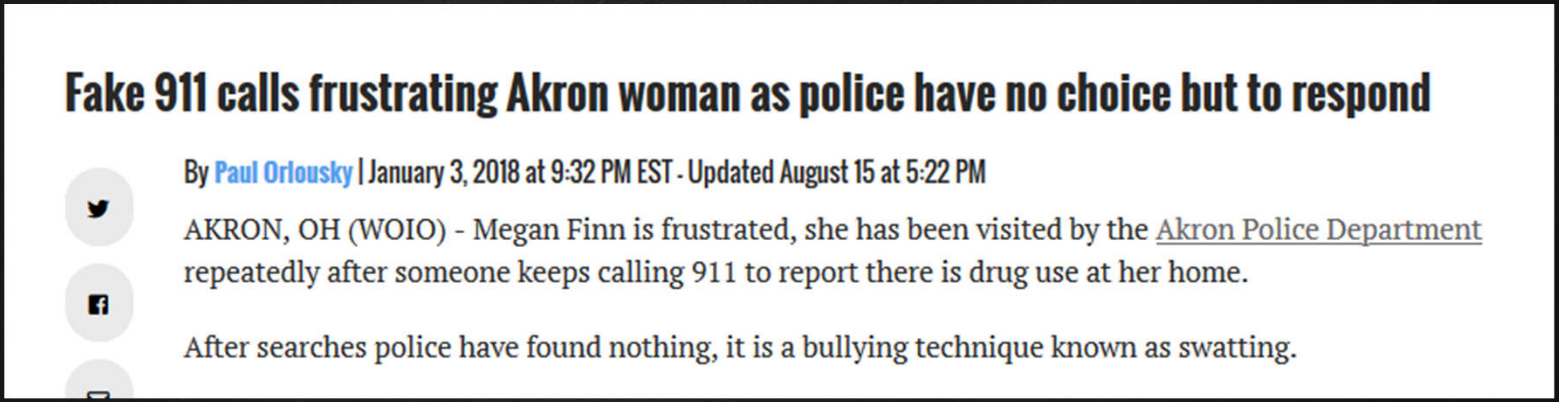
SWATTING/PRANK/HOAX 9-1-1 CALLS



TTY RELAY

VoIP

HARASSMENT/BULLYING



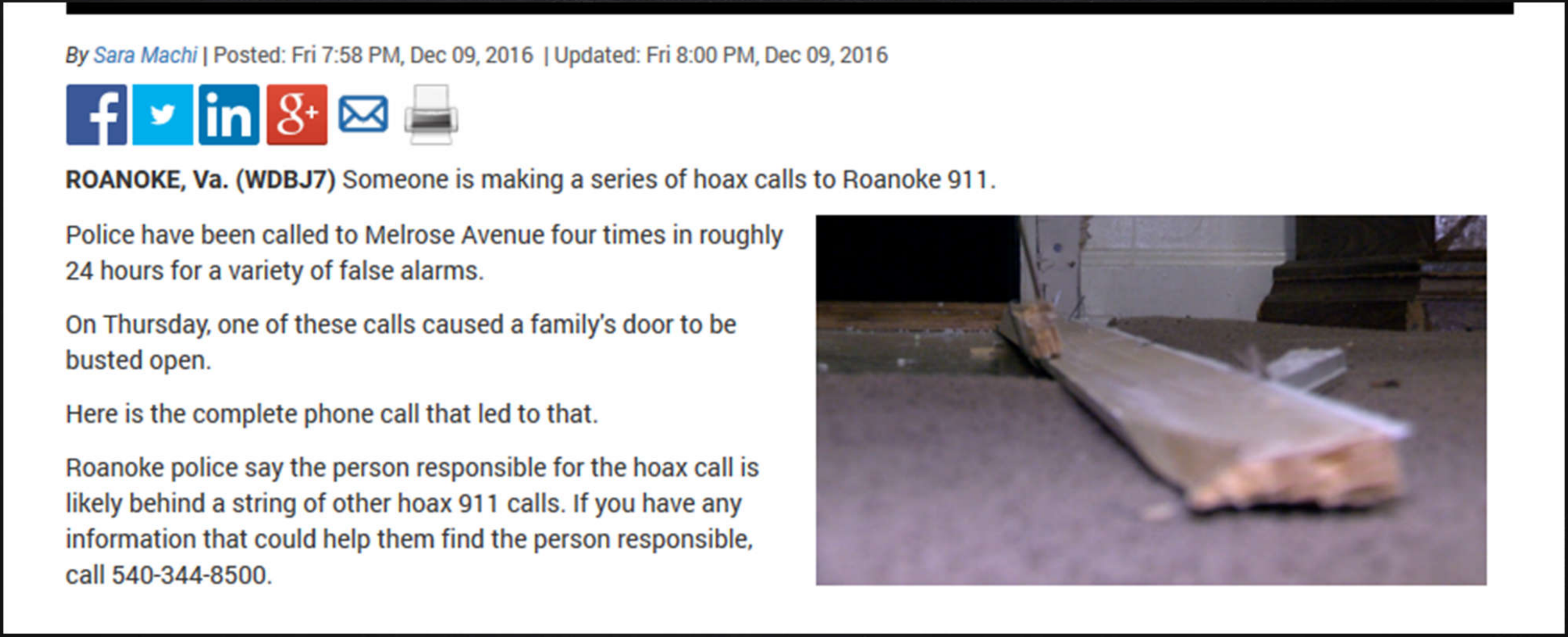
Fake 911 calls frustrating Akron woman as police have no choice but to respond

By Paul Orlousky | January 3, 2018 at 9:32 PM EST - Updated August 15 at 5:22 PM

AKRON, OH (WOIO) - Megan Finn is frustrated, she has been visited by the Akron Police Department repeatedly after someone keeps calling 911 to report there is drug use at her home.

After searches police have found nothing, it is a bullying technique known as swatting.

RESULTS IN PROPERTY DAMAGE



By Sara Machi | Posted: Fri 7:58 PM, Dec 09, 2016 | Updated: Fri 8:00 PM, Dec 09, 2016

ROANOKE, Va. (WDBJ7) Someone is making a series of hoax calls to Roanoke 911.

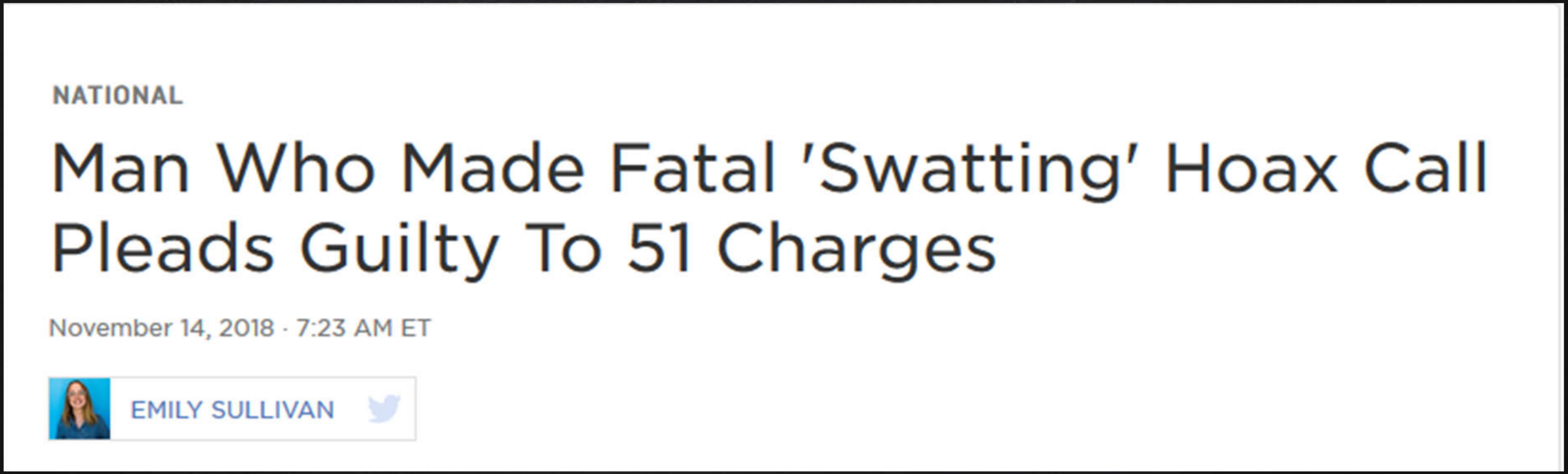
Police have been called to Melrose Avenue four times in roughly 24 hours for a variety of false alarms.

On Thursday, one of these calls caused a family's door to be busted open.

Here is the complete phone call that led to that.

Roanoke police say the person responsible for the hoax call is likely behind a string of other hoax 911 calls. If you have any information that could help them find the person responsible, call 540-344-8500.

DEATH OF CITIZEN OR FIRST RESPONDER



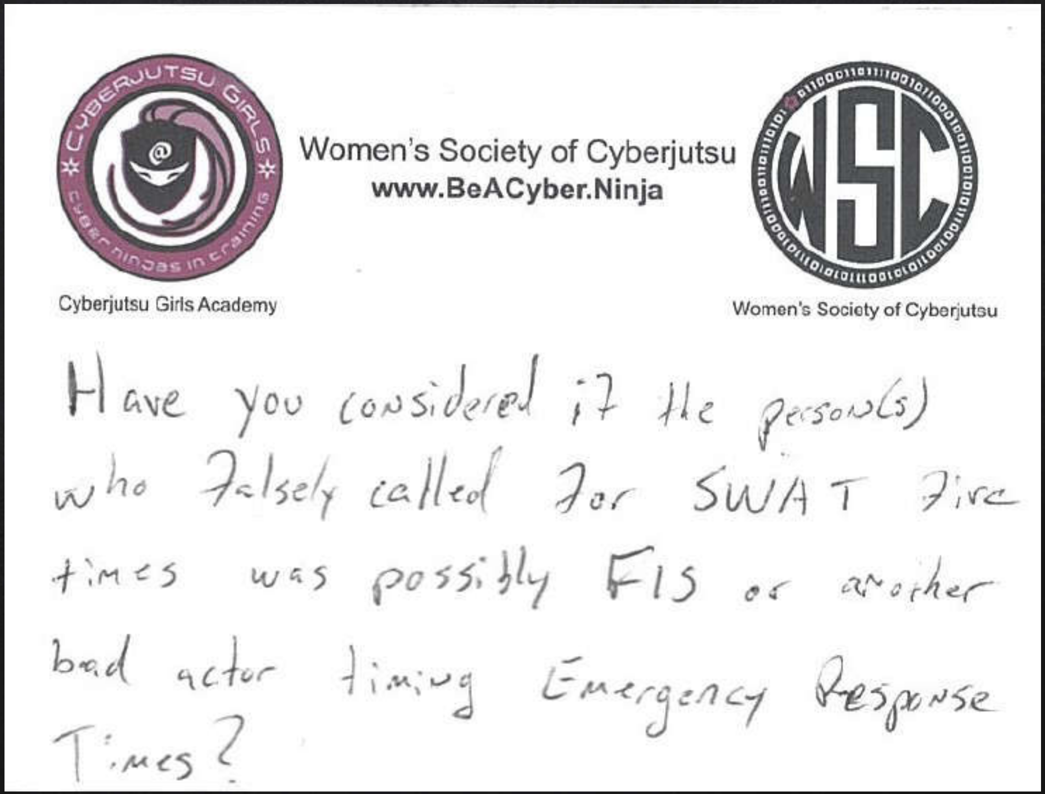
NATIONAL

Man Who Made Fatal 'Swatting' Hoax Call Pleads Guilty To 51 Charges

November 14, 2018 · 7:23 AM ET

EMILY SULLIVAN

INTERESTING QUESTION



Cyberjutsu Girls Academy

Women's Society of Cyberjutsu
www.BeACyber.Ninja

Women's Society of Cyberjutsu

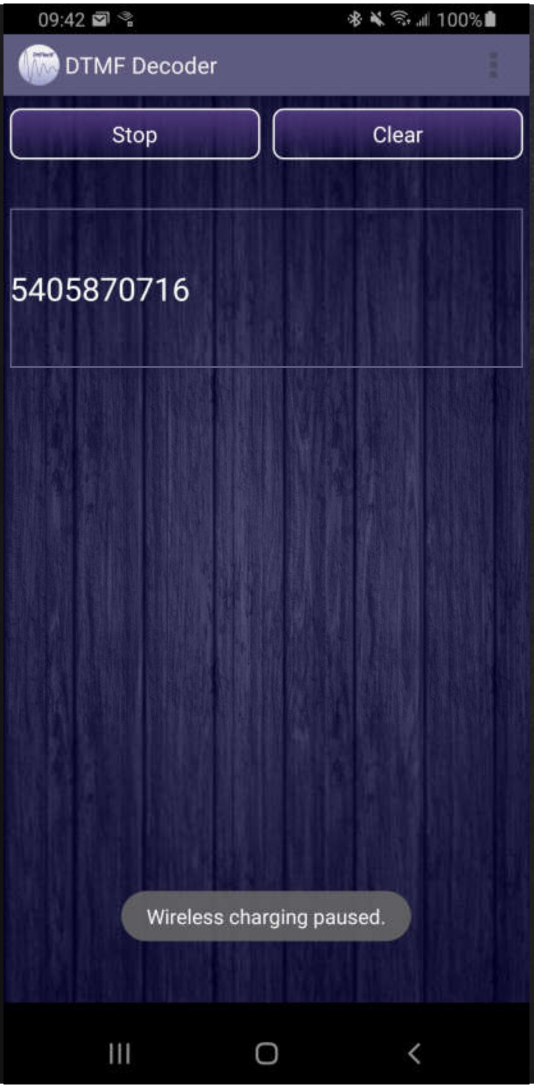
Have you considered if the person(s) who falsely called for SWAT five times was possibly FIS or another bad actor timing Emergency Response Times?

**

AUDIO FROM FOIA REQUEST

- Decoding DTMF (dual tones multifrequency) to obtain outgoing phone number
- Decoding FSK Caller ID (frequency shift keying) to determine incoming phone number

**



5405870716

Wireless charging paused.

DTMF DECODING

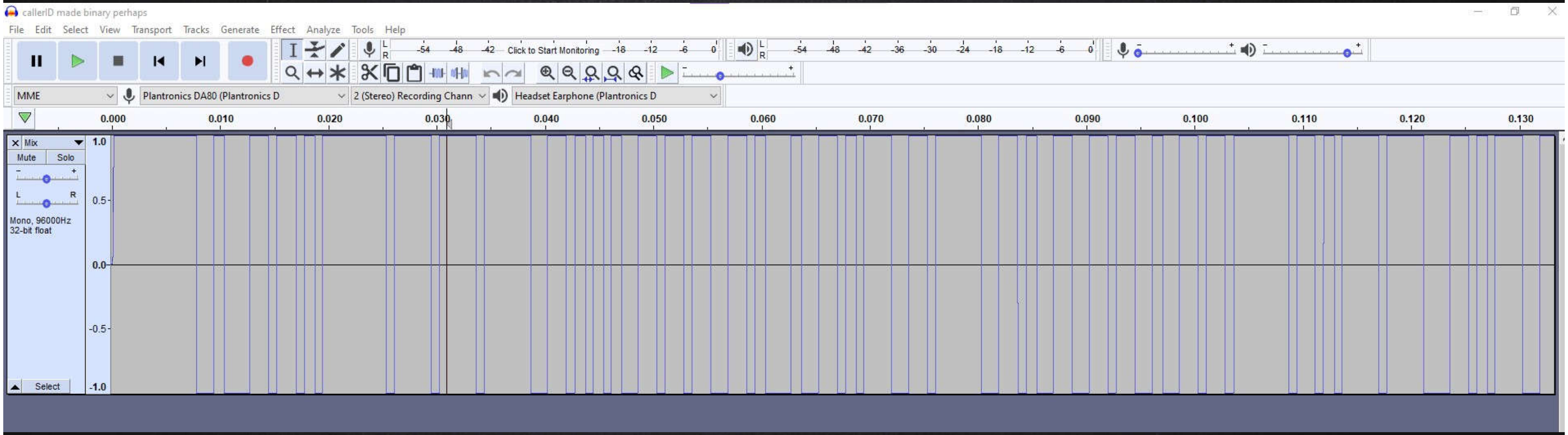
- Use a free app on cell phone
- Multimon-NG on the computer

**

DECODING FSK CALLERID

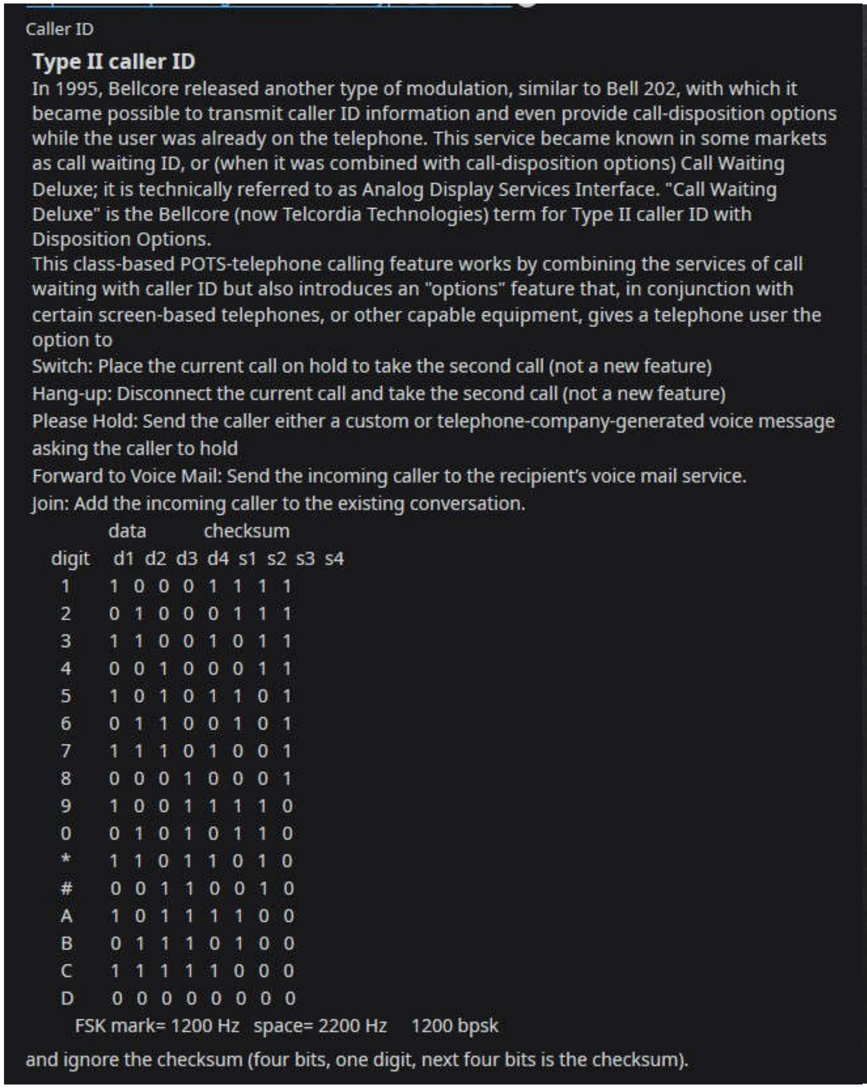
- Can be done manually (very tedious)
- Can be done with software called Minimodem

MANUAL


callerID made binary perhaps
File Edit Select View Transport Tracks Generate Effect Analyze Tools Help
Click to Start Monitoring
MME
Plantronics DA80 (Plantronics D
2 (Stereo) Recording Chann
Headset Earphone (Plantronics D
0.000
0.010
0.020
0.030
0.040
0.050
0.060
0.070
0.080
0.090
0.100
0.110
0.120
0.130
Mix
Mute
Solo
Mono, 96000Hz
32-bit float
Select
1.0
0.5
0.0
-0.5
-1.0

APPLICATION USED: Audacity (FREE)

MANUAL



Caller ID

Type II caller ID

In 1995, Bellcore released another type of modulation, similar to Bell 202, with which it became possible to transmit caller ID information and even provide call-disposition options while the user was already on the telephone. This service became known in some markets as call waiting ID, or (when it was combined with call-disposition options) Call Waiting Deluxe; it is technically referred to as Analog Display Services Interface. "Call Waiting Deluxe" is the Bellcore (now Telcordia Technologies) term for Type II caller ID with Disposition Options.

This class-based POTS-telephone calling feature works by combining the services of call waiting with caller ID but also introduces an "options" feature that, in conjunction with certain screen-based telephones, or other capable equipment, gives a telephone user the option to

Switch: Place the current call on hold to take the second call (not a new feature)

Hang-up: Disconnect the current call and take the second call (not a new feature)

Please Hold: Send the caller either a custom or telephone-company-generated voice message asking the caller to hold

Forward to Voice Mail: Send the incoming caller to the recipient's voice mail service.

Join: Add the incoming caller to the existing conversation.

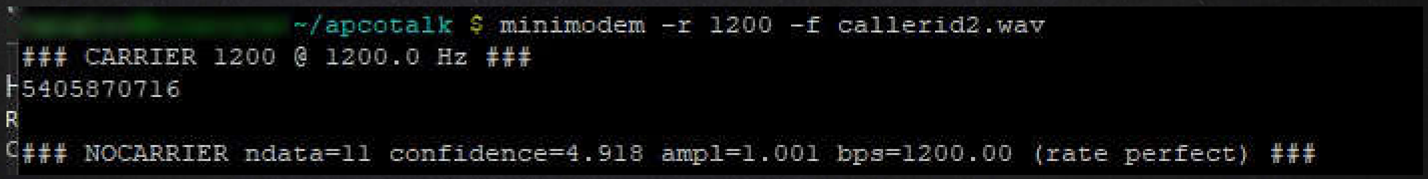
	data				checksum			
digit	d1	d2	d3	d4	s1	s2	s3	s4
1	1	0	0	0	1	1	1	1
2	0	1	0	0	0	1	1	1
3	1	1	0	0	1	0	1	1
4	0	0	1	0	0	0	1	1
5	1	0	1	0	1	1	0	1
6	0	1	1	0	0	1	0	1
7	1	1	1	0	1	0	0	1
8	0	0	0	1	0	0	0	1
9	1	0	0	1	1	1	1	0
0	0	1	0	1	0	1	1	0
*	1	1	0	1	1	0	1	0
#	0	0	1	1	0	0	1	0
A	1	0	1	1	1	1	0	0
B	0	1	1	1	0	1	0	0
C	1	1	1	1	1	0	0	0
D	0	0	0	0	0	0	0	0

FSK mark= 1200 Hz   space= 2200 Hz   1200 bpsk

and ignore the checksum (four bits, one digit, next four bits is the checksum).

Use table shown to decode (available anywhere online)

MINIMODEM

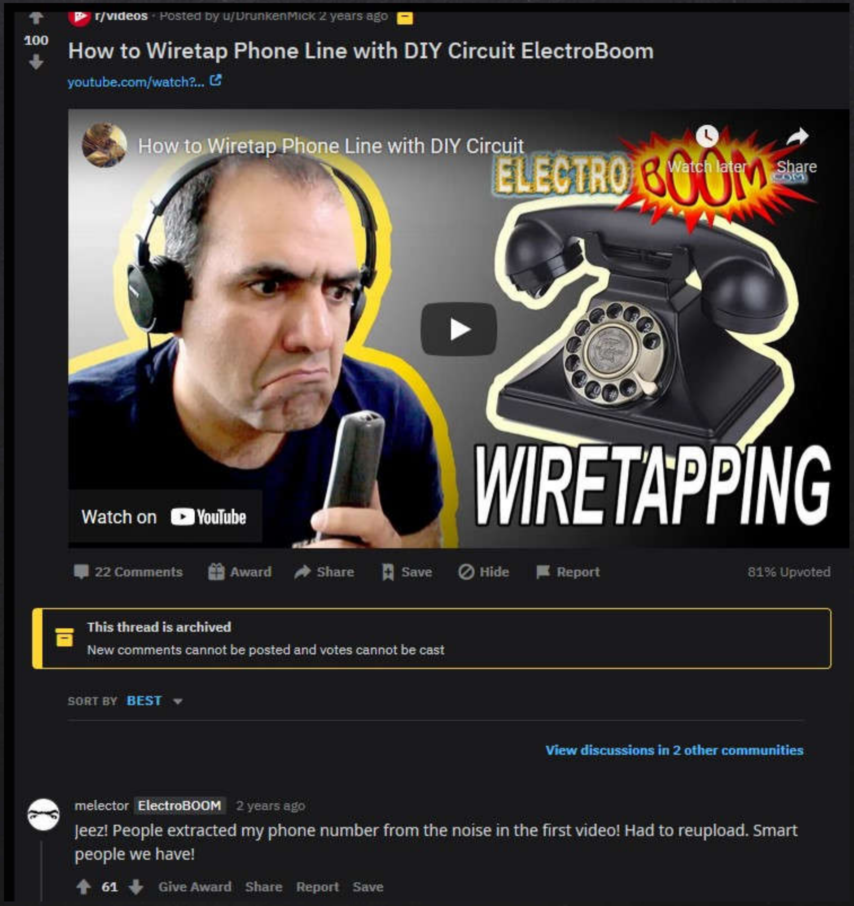


```
[redacted] ~/apcotalk $ minimodem -r 1200 -f callerid2.wav
### CARRIER 1200 @ 1200.0 Hz ###
5405870716

### NOCARRIER ndata=11 confidence=4.918 ampl=1.001 bps=1200.00 (rate perfect) ###
```

APPLICATION USED: Minimodem (FREE)

IN THE WILD



r/videos · Posted by u/DrunkenMick 2 years ago

100

How to Wiretap Phone Line with DIY Circuit ElectroBoom

youtube.com/watch?...

22 Comments Award Share Save Hide Report 81% Upvoted

This thread is archived
New comments cannot be posted and votes cannot be cast

SORT BY BEST

View discussions in 2 other communities

melector ElectroBOOM 2 years ago

Jeez! People extracted my phone number from the noise in the first video! Had to reupload. Smart people we have!

61 Give Award Share Report Save

911 LINE PREAMBLE

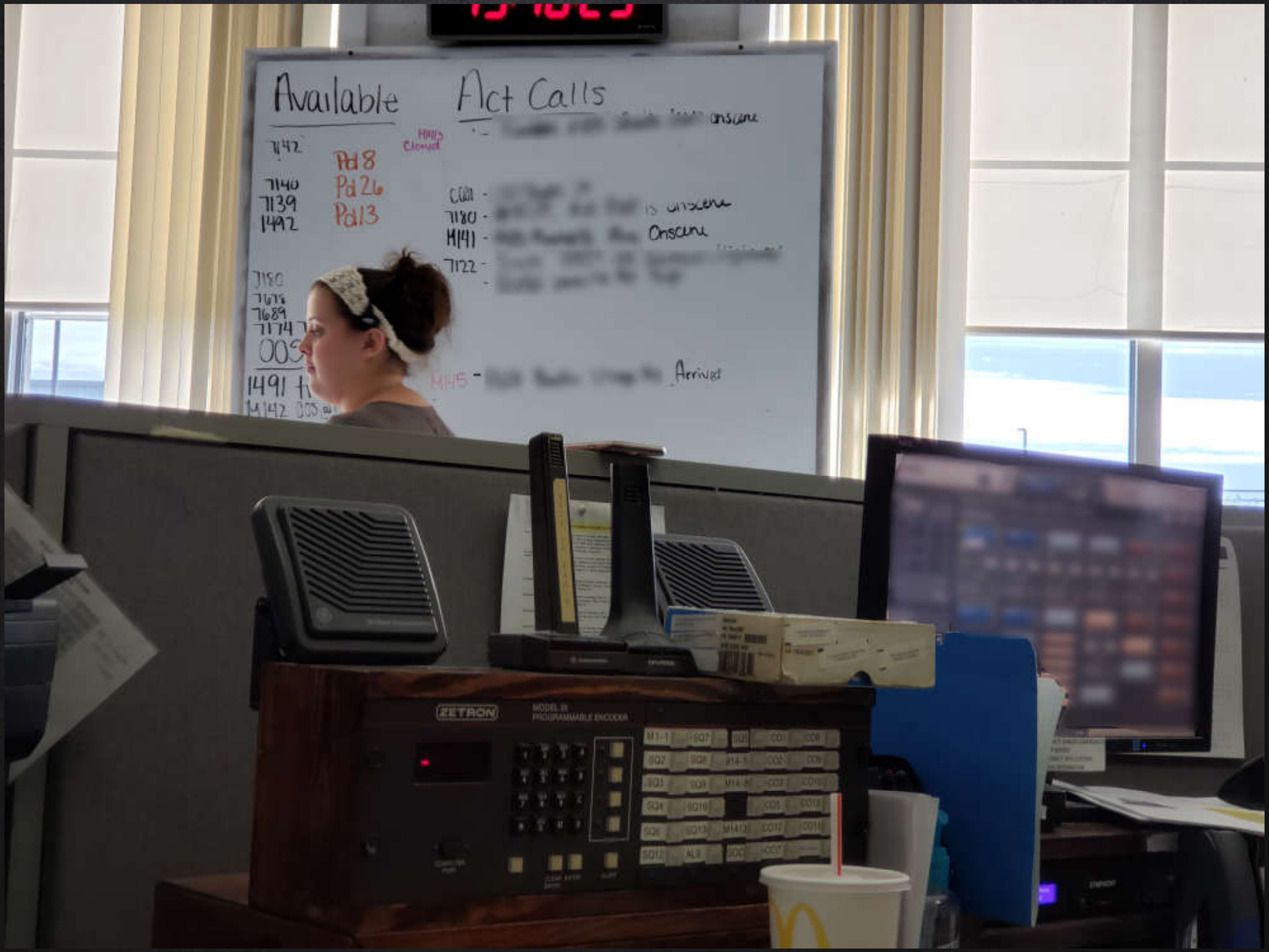
ANI tone drop

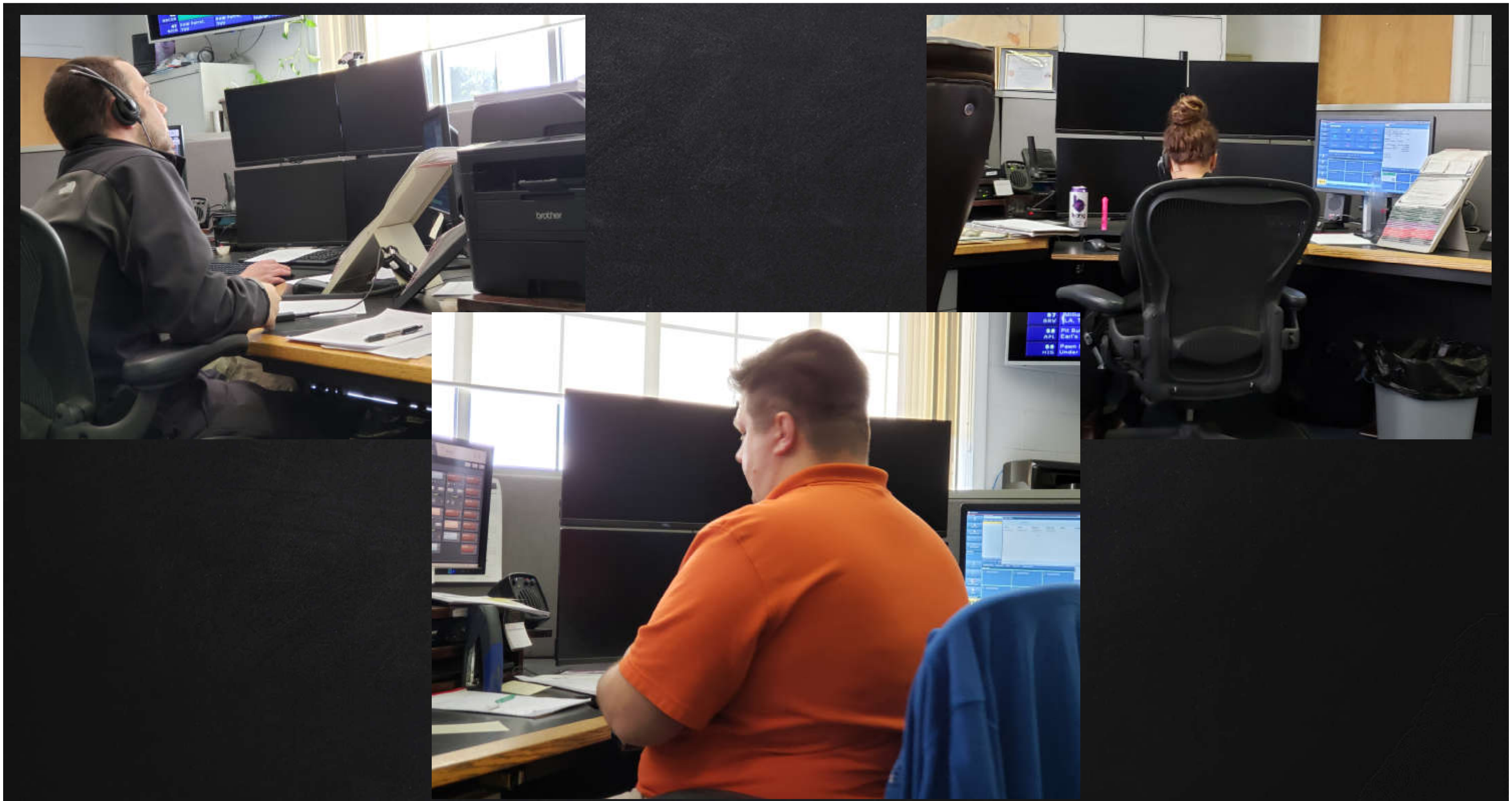
This is so that the system can location the number in the ALI database

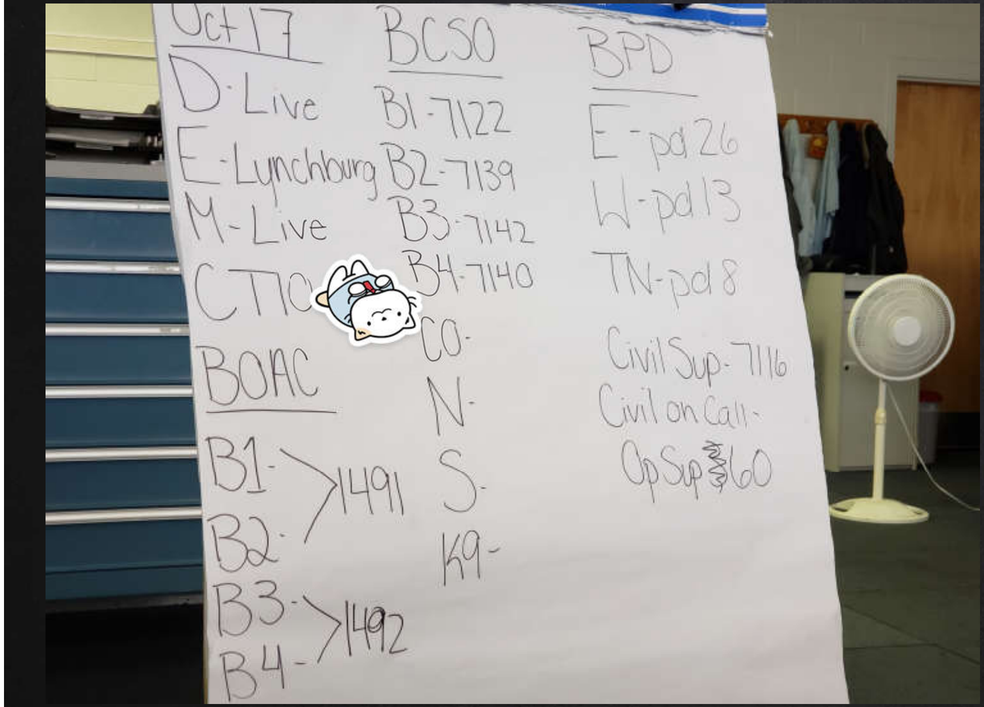
DARK OCTOBER 2019

WE WERE HIT WITH RANSOMWARE

- Came in over e-mail
- We had anti-virus
- Took out the systems within 10 minutes
- I don’t want to do it again, but it was fun!


Available
Act Calls
onscene
7142
7140
7139
1492
Pd 8
Pd 26
Pd 13
C601
7180
M141
7122
Onscene
7180
1491
M142
M145
Arrived
ZETRON
MODEL 35 PROGRAMMABLE ENCODER





Oct 17

D-Live
E-Lynchburg
M-Live
CTIC

BOAC

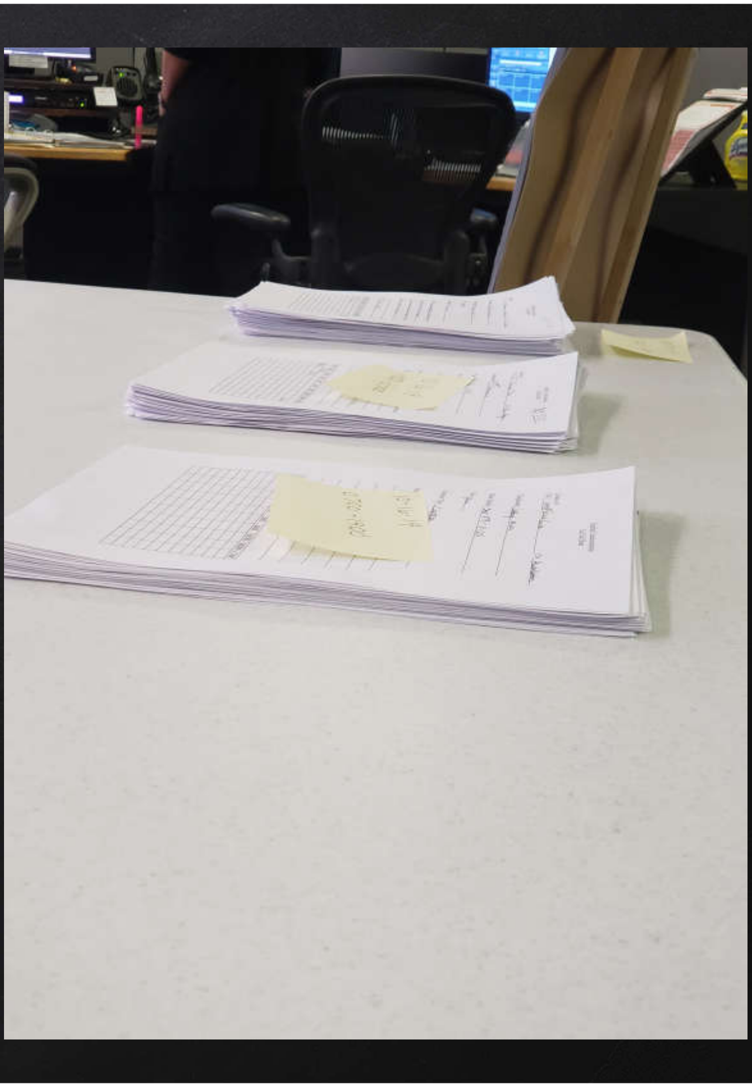
B1- > 1491
B2-
B3- > 1492
B4-

BCSO

B1-7122
B2-7139
B3-7142
B4-7140
CO-
N-
S-
K9-

BPD

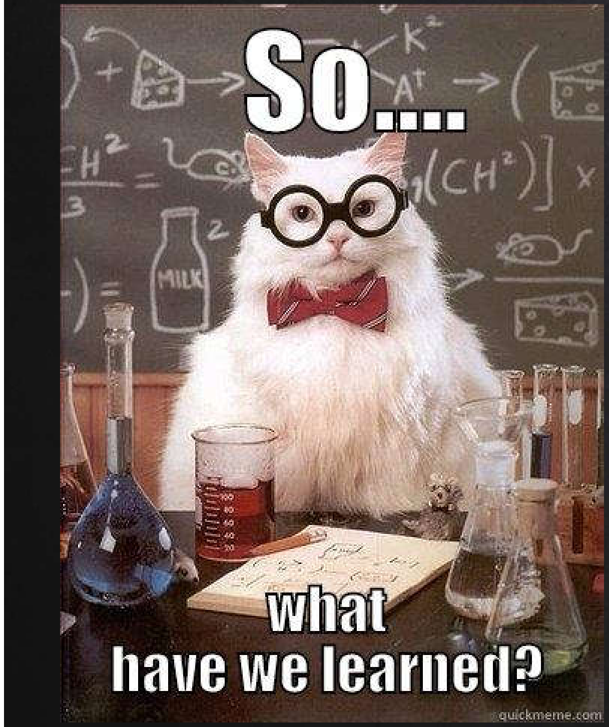
E-pd 26
W-pd 13
TN-pd 8
Civil Sup-7116
Civil on Call-
Op Sup 60



RANSOMWARE SURVEY RESULTS

https://www.surveymonkey.com/r/ZDZ75XM

- 25% were hit with ransomware more than once
- 66 % weren’t able to use CAD
- Times to full functionality restoration were 2 days to several months.
- All attack vectors were e-mail except one which was RDP vulnerability
- long lasting losses/issues due to ransomware



- ✓ Don’t pay the ransom
- ✓ Make sure to have good backups and test regularly
- ✓ E-mail attachments and links
- ✓ Continued education of users
- ✓ Turn on 2 factor and secure 2 factor device
- ✓ Quarterly audit of accounts access and need
- ✓ Remove/disable inactive accounts immediately

THANK YOU!

https://bedford911.com/handout/

Contact information
cgiglio@bedfordcountyva.gov
https://www.linkedin.com/in/ctgiglio/
Phone: 540-587-0716