911 SWATting Webinar

An Introduction and Overview

NATIONAL 911 PROGRAM

SEPTEMBER 15, 2015

911.gov

National 911 Program’s Webinar Series

Designed to provide useful information about Federal and State participation in the planning, design, and implementation of Next Generation 911 (NG911) coupled with real experiences from leaders overseeing these transitions throughout the country.

This webinar focuses on increasing awareness of SWATting incidents for the 911 community and discusses steps toward preparedness and response.

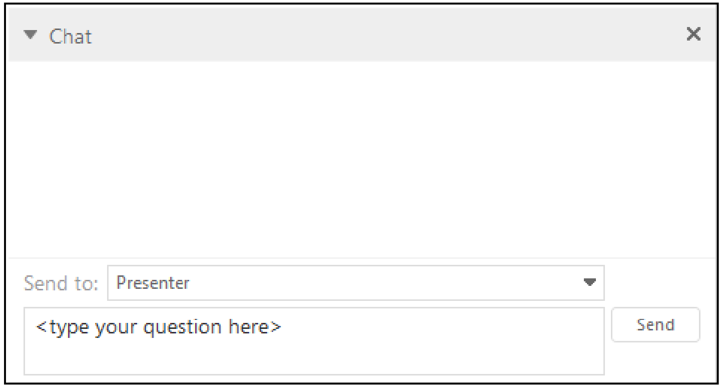
For more information on future webinars, access to archived recordings and to learn more about the National 911 Program, please visit 911.gov

Feedback or questions can be sent to: National911Team@mcp911.com

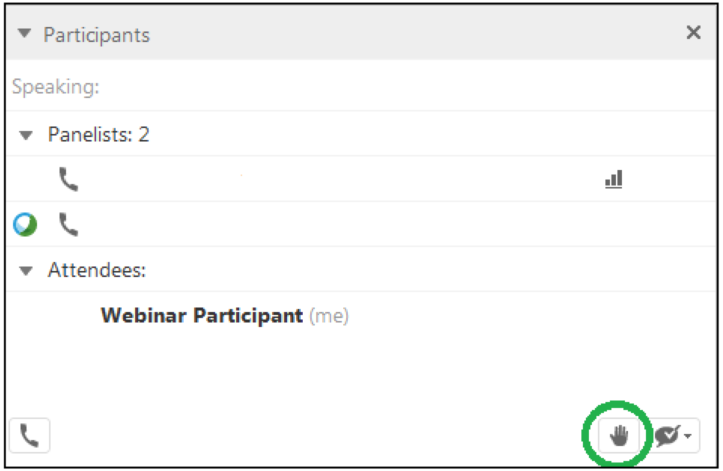
Questions?

For WebEx Technical Assistance, please call: (866) 229-3239, Option 1

To ask a question, please use WebEx's "Chat" feature located on the right-hand side of your screen.



During the Q&A portion of the webinar, please click on "Raise Hand" and your phone will be unmuted.



An Introduction to SWATting

CHRISTOPHER BLAKE CARVER, ENP, RPL

DIRECTOR – PSAP OPERATIONS

NATIONAL EMERGENCY NUMBER ASSOCIATION (NENA)

What is “SWATting?”

From the prospective of a 9-1-1 Center, SWATting is the deliberate reporting of a serious event, normally police related, intended to cause embarrassment or discomfort to someone.

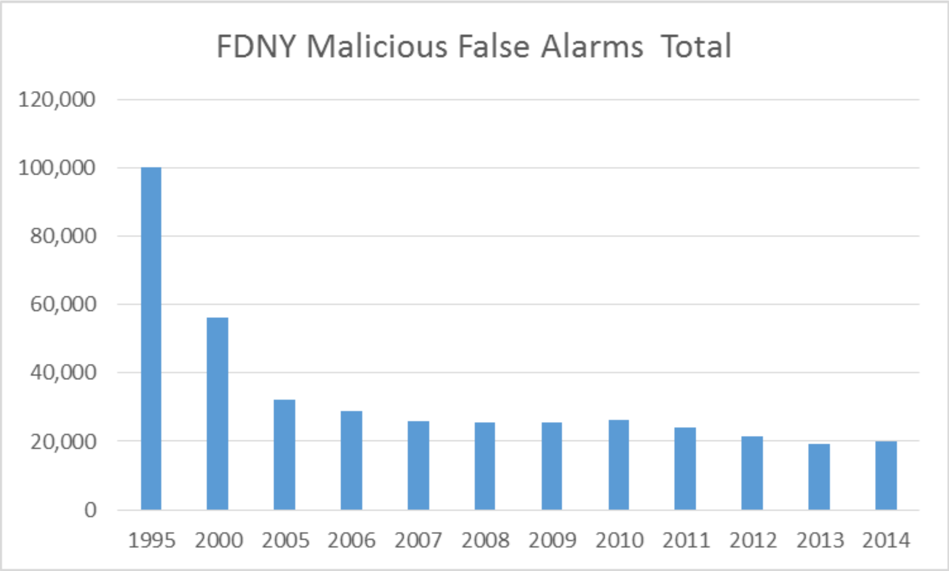
Recent popularity started in the gaming community, as gamers called in false reports on other gamers for various reasons.

Given that these reports would come from potentially very far away from the location of the reported incidents, perpetrators needed to figure out how to get into the necessary 9-1-1 agency to make the report.

But this really isn't new

False Alarms have been around as long as there have been phones and call boxes available to report emergencies.

NYC is just one example of a place that has experienced them.



This is how common they have been…

A first-season episode of the popular TV police show CHiPs, addressed the issue of false alarms in 1978.

A troubled youth utilized highway call-boxes to report large scale disasters that generated massive emergency responses.

But why is it different now?

- Technology
- Severity
- Climate and Culture

All of these factors contribute to Swatting being very dangerous.

The reality is there is relatively little the 9-1-1 center can do

However, there are strategies available to lessen the danger posed by these events.

Follow call handling policies and share with responders if you have reason to believe it to be a “SWATting event”

- Major emergency reported with one phone call on a non-emergency line
- A single call for an incident that should have many
- No ability to verify the information (caller unwilling to provide any information)
- Premise history information indications
- Dispatchers should be encouraged to use their skills, training, and intuition to provide the best possible information to responders.

Other PSAP Actions

Ensure Supervisors are made aware of the event

Enter SWATting events into the incident address history

Obtain as much information as possible from the caller– may permit easier identification if/when a court case occurs

Why can't we just ignore calls we know to be false?

- More examples than we can list here of calls where it was assumed to be a false alarm and it wasn't
- So then what is the best approach to prevent these?

Strict enforcement and punishment

From the 9-1-1/PSAP prospective; the best deterrence to SWATting is very strict enforcement and strong punishment.

The “gaming” community is a social media network. Word will get around as stricter legislation is passed and people are caught.

Thankfully, that approach has been proven to work. The rate of malicious false alarms in NYC dropped dramatically, in large part due to enforcement and public awareness of the “cost” of such responses.

For a prospective from the “tech side”, we now turn the presentation over to Mark Fletcher.

The Mechanics of SWATting

MARK J. FLETCHER, ENP

CHIEF ARCHITECT – WORLDWIDE PUBLIC SAFETY SOLUTIONS

SWAT Attack vs. Social Engineering

SWATting via Attack on the Network:

Call on a 911 Trunk while spoofing ANI – ***Tricking the System***

- While possible – *Often not feasible without complex equipment*
- While possible – *Often difficult from remote 911 Service Areas*

REALITY CHECK: Difficult to identify – Difficult to Prevent

SWATting via Social Engineering:

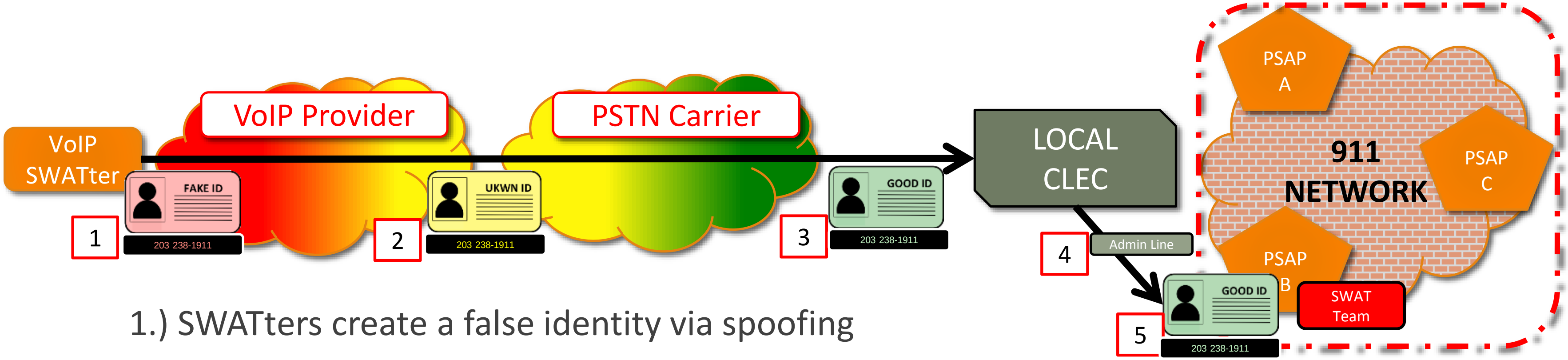
Calls on 'Administrative Lines' for a major event

Obvious spoofed ANI or Caller ID

- Blocked Number - (000) 000-0000 – Familiar or your own number

REALITY CHECK: Identified and Minimized through Awareness Programs & Government Security Hack-a-thons

Unintentional Validation of Identity



1.) SWATters create a false identity via spoofing

2.) VoIP Providers pass calls to carriers – Little to no validation

3.) Carriers accepts calls as validated and pass traffic to CLEC – no verification indicator

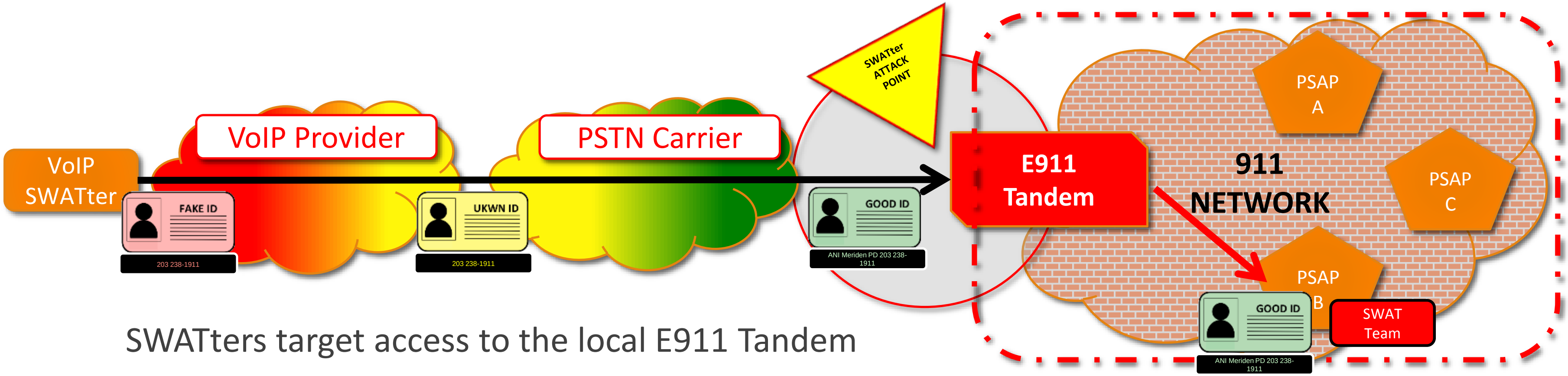
4.) Local PSTN delivers the call with assumption Caller ID is valid

5.) Social Engineering tactics are used against the ‘human element“ in the network

THERE IS NO BREECH OF SECURITY ON THE 9-1-1 NETWORK

Spoofing the 911 Network

More Difficult – But NOT Impossible



SWATters target access to the local E911 Tandem

Calls not meeting ANI criteria can fall out and DEFAULT ROUTE – **ⓘWARNING SIGNⓘ**

Very difficult without explicit knowledge of the infrastructure therefore:

- Protect your recordings by redacting call delivery and transfer tones
- Protect circuit ID’s and account information with the highest level of security
- Treat your network and configuration like keys to your house – **STRICT NEED TO KNOW ACCESS**

In the hands of a SWATter, they can map out an attack your network

Be Aware - Social Engineering Attempts

Single call event on a major incident

- While not impossible, it's unlikely that a SWATter will be able to simulate the call volume indicative with large scale incidents
- Respond but be suspect of incidents that do not match normal call volume profiles

Track NSI ANI received on devices/incidents – SHARE THIS INFORMATION

- The ESN / IEMI is a unique identifier on the device
- If it is the same NSI ANI – It is likely the same device

Place calls to a suspected Spoofed number while the call is active

- Busy?
- Voice Mail?
- Someone answers while talking to the original caller?
- **Be sure to use an unlisted number or line**
- **Don't tip off your suspect!**

- CALL WAITING -
Meriden Police Dept.
(203) 238-1911

NSI Devices **have** a Fingerprint

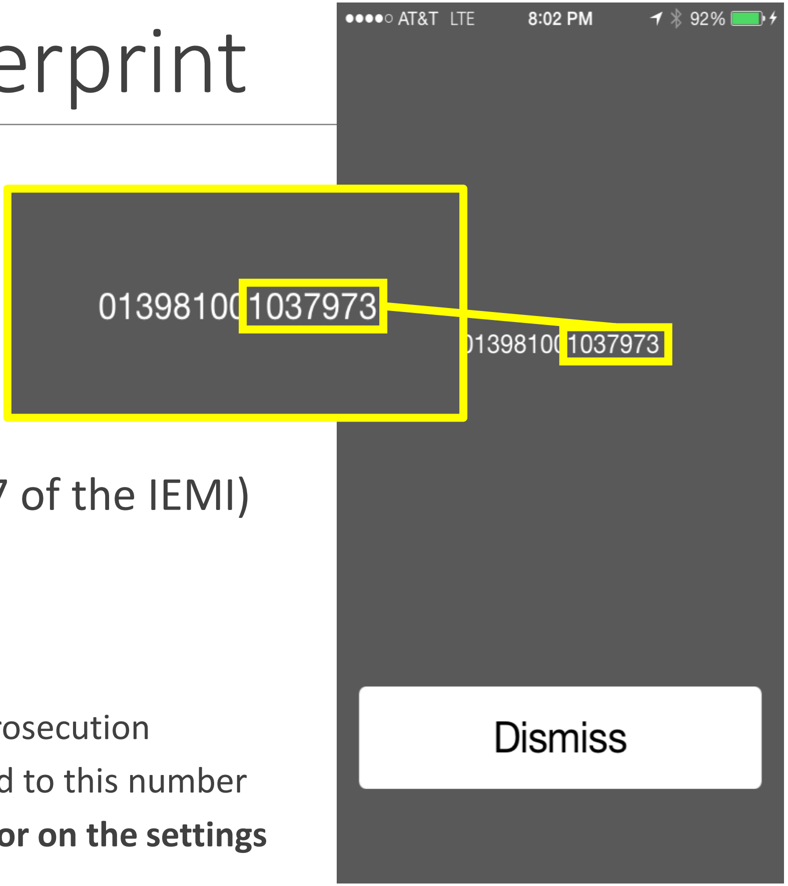
A Typical NSI “Burner Phone” will have:

- No carrier account plan
- No SIM card
- YET, these phones are NOT completely anonymous

NSI Phones use 911-XXX-XXXX as the ANI (X = last 7 of the IEMI)

This NSI Phone will show the ANI of ***911-103-7973***

- The **103-7973** are the last 7 digits of the IMEI (International Mobile Equipment Identity)
- This is critical information that can be valuable evidence for prosecution
- If a suspect is captured, the IMEI on the phone can be matched to this number
- **Simple to display the IMEI on many phones by dialing *#06# or on the settings menu (About this Device)**



013981001037973

Current FCC NPRM for NSI Phones

PART 20 – COMMERCIAL MOBILE RADIO SERVICES

1. Section 20.18 is amended by revising paragraph (b) and adding paragraph (l)(4), to read as follows:

(b) *Basic 911 Service*. CMRS providers subject to this section must transmit all wireless 911 calls without respect to their call validation process to a Public Safety Answering Point, or, where no Public Safety Answering Point has been designated, to a designated statewide default answering point or appropriate local emergency authority pursuant to § 64.3001 of this chapter, provided that “all wireless 911 calls” is defined as “any call initiated by a wireless user dialing 911 on a phone using a compliant radio frequency protocol of the serving carrier.”

After [Date of Order plus 6 months], the requirements of this section will no longer apply to calls from non-service-initialized handsets as defined in paragraph (l)(3)(i) of this section.

Spoofing Services Openly Advertised

Simple GOOGLE searches for “spoofing” will result in several companies that provide this service for VALID REASONS, however they have no control over the use of the service for illicit purposes.

Unfortunately, some product positioning seems to promote this:

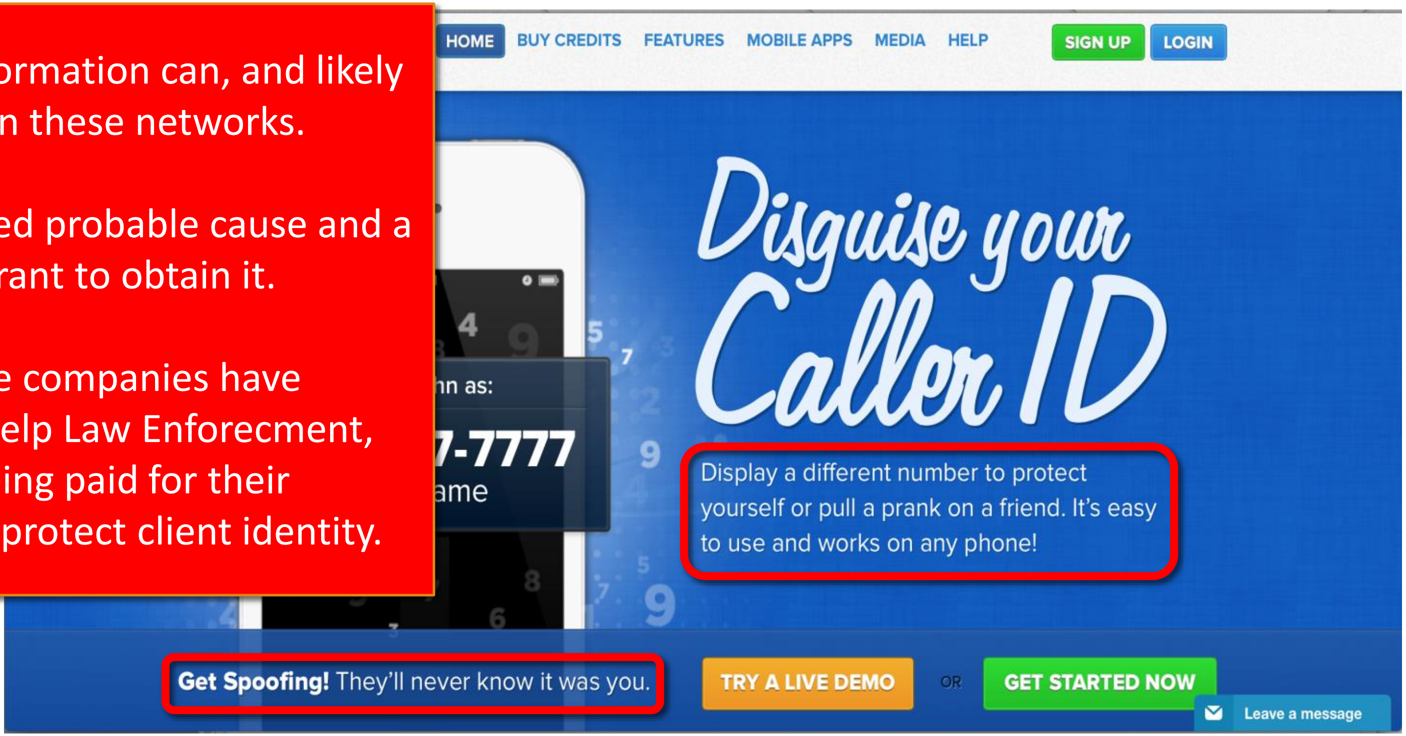
> *Our service is intended for business professionals within the U.S. including, but not limited to; Private Investigators, Skip Tracers, Law Enforcement and Lawyers, giving them freedom to* ***choose any number as the Caller ID.*** ***XXXXXXXX allows you to be whoever you want to be.***

Ease of Access increases use

IP trace information can, and likely does exist in these networks.

You will need probable cause and a search warrant to obtain it.

While these companies have vowed to help Law Enforecment, they are being paid for their services to protect client identity.



Display a different number to protect yourself or pull a prank on a friend. It's easy to use and works on any phone!

Get Spoofing! They'll never know it was you.

Breadcrumbs - Finding the Bad Guy

In order to SWAT, you need to access the PSTN or 9-1-1 Network. This is accomplished via voice access or internet access.

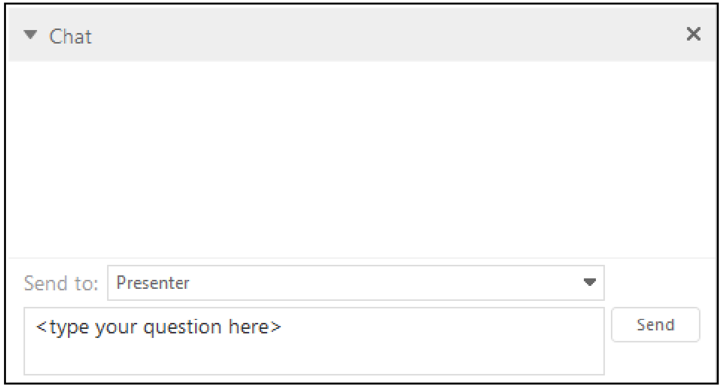
Both can leave tell tale breadcrumbs as evidence. Using data forensics and network IP Tracing can be used like fingerprints. However, you need a suspect to look for a match. This is where trace evidence needs to be collected, and shared.

Locking the door is no longer sufficient.

Public Safety requires a new level of education around network security tactics to understand how the bad guys are working the network to their advantage.

Q&A Period

WebEx's "Chat" feature located on the right-hand side of your screen.



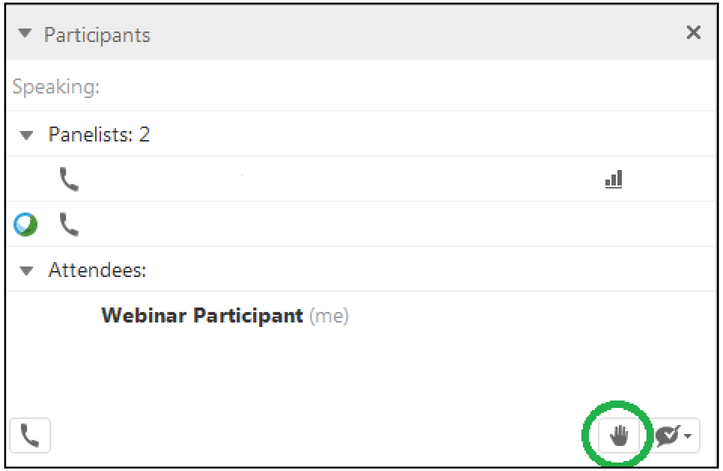
Chat

Send to: Presenter

<type your question here>

Send

Click on "Raise Hand" and your phone will be unmuted.



Participants

Speaking:

Panelists: 2

Attendees:

Webinar Participant (me)

SWATting Resources / Info

Downloadable resource: http://www.911.gov/pdf/PublicSafetyInfo-Swatting-may2015.pdf

FCC Workshop to Focus on Robocall Blocking and Caller ID Spoofing

TOMORROW: Wednesday, 9/16 – 9:00 AM - 3:00 PM EDT

Watch live: https://www.fcc.gov/live

Future Webinars

Next Scheduled Webinar: **Tuesday, October 13, 2015 at 12 noon ET**

Presenters will include:

- Mr. Richard (Dick) Tenney, Deputy, Technical Assistance Branch, DHS Office of Emergency Communications (OEC)
- Ms. Cheryl Benjamin, Street and Address Maintenance Program, NYS Office of Information Technology Services

Visit 911.gov to access archived webinars

National 911 Program

Laurie Flaherty

Program Coordinator

202-366-2705

laurie.flaherty@dot.gov

Feedback or questions can be sent to: National911Team@mcp911.com