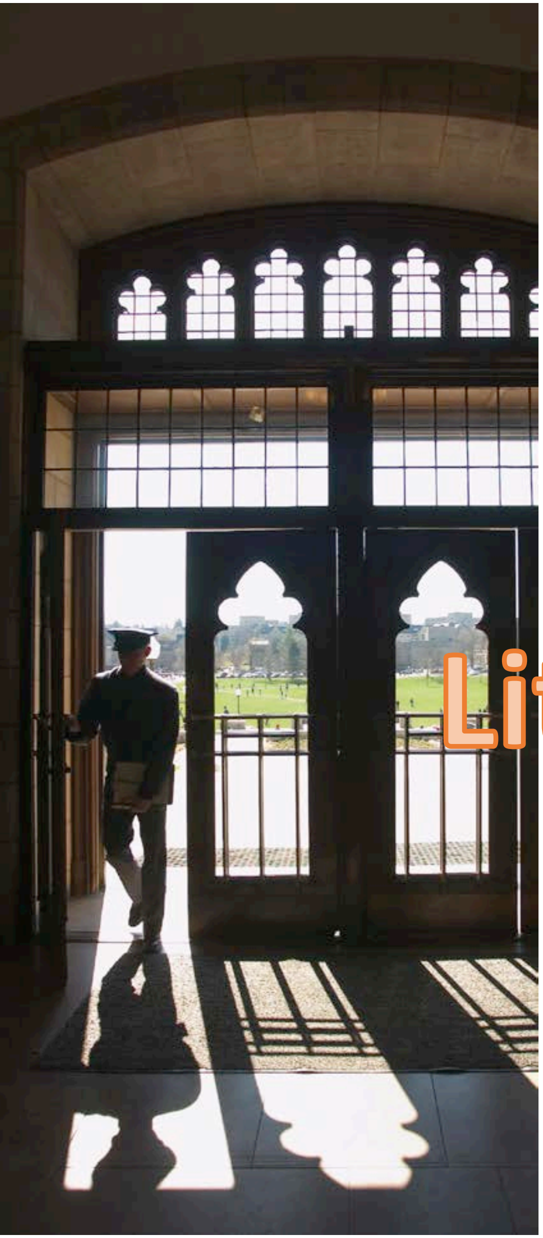
Security & The Internet of Things

Randy Marchany

Virginia Tech IT Security Office and Lab



What? Worry? Me?

- Internet of Things (IoT) is the latest phase in computer technology
- Computers embedded in common devices AND connected to the Internet
  - Lab equipment
  - Cash registers
  - Building control
    - Thermostats, lights, plumbing
  - Autos, trucks
  - Everyday devices (TV, toasters, etc.)

Little or NO Security yet can handle sensitive data

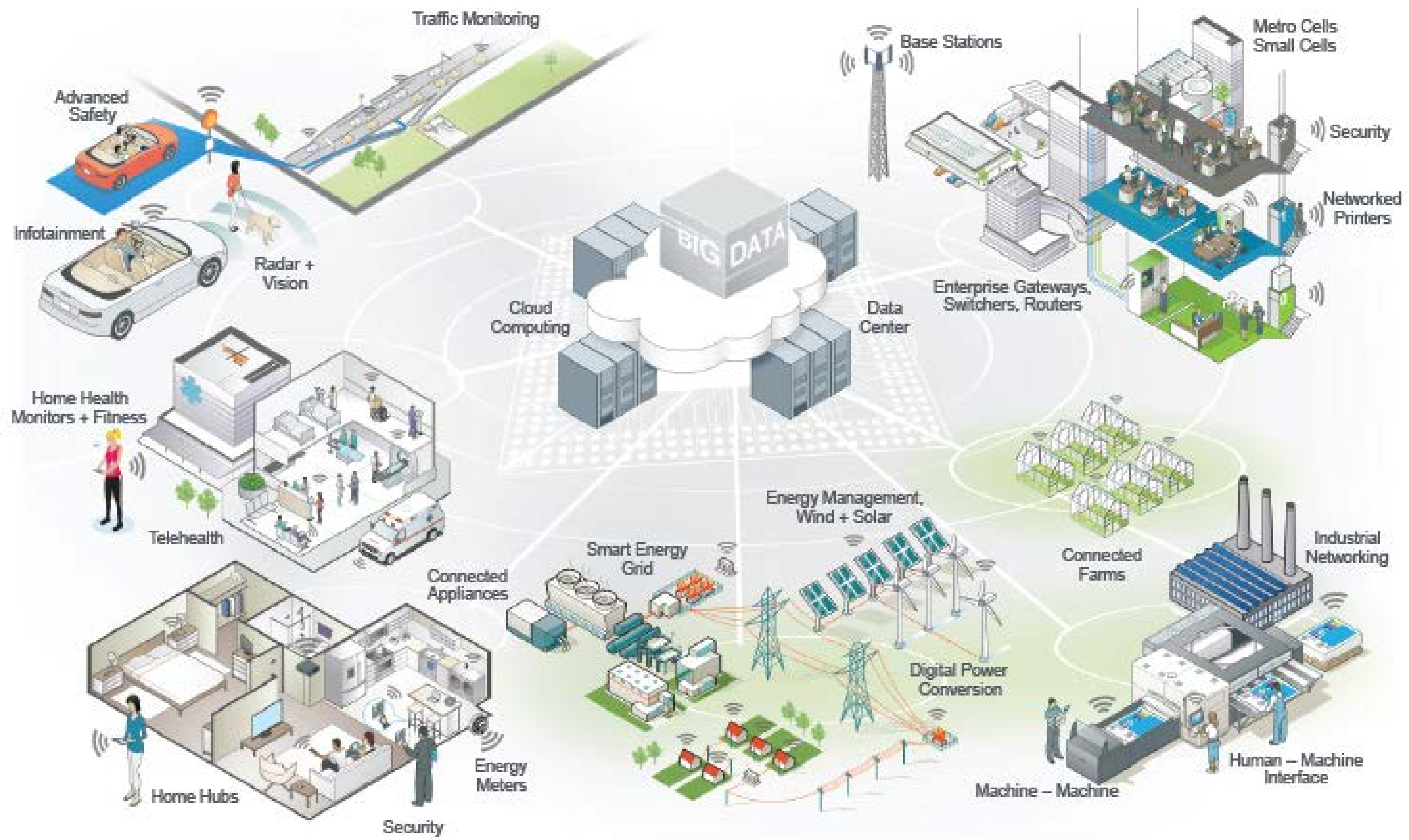
Internet of Things (IoT) Examples

- https://www.postscapes.com/internet-of-things-examples
- https://www.youtube.com/watch?v=QSIPNhOiMoE
- https://www.youtube.com/watch?v=u1ymmRQ_p3k

- IoT is pervasive in the home and the workplace
- Need to carefully examine the implications of having such devices in the workplaces

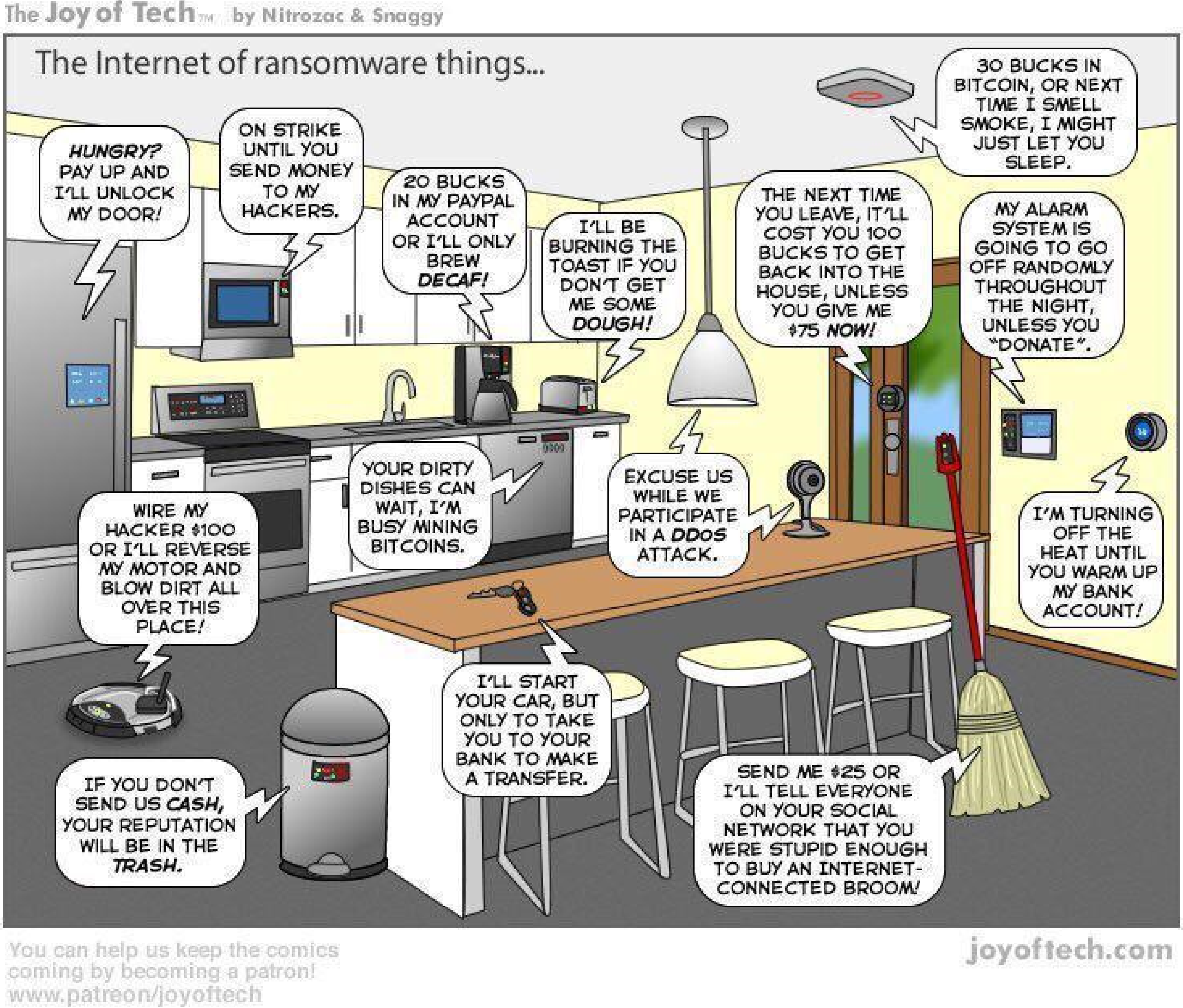
- Security features are NOT built into IoT

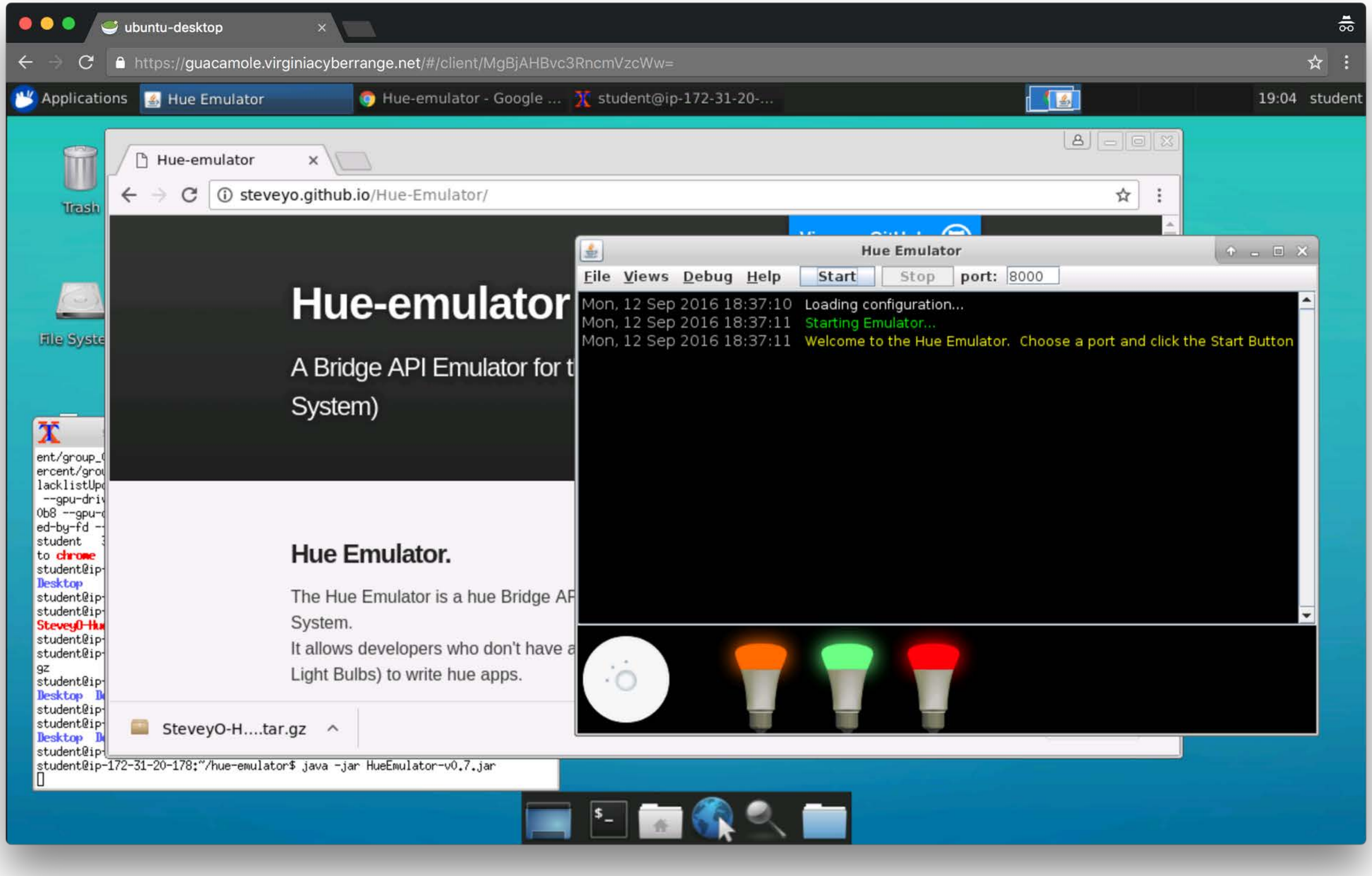
ENABLING SMART CONNECTED SOLUTIONS FROM THE END NODE TO THE CLOUD



How IoT Got Hacked

- https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/
- https://www.youtube.com/watch?v=Ct3NJWq0LgE
  Hacking the Internet of Things


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com



Hue-emulator

A Bridge API Emulator for t
System)

Hue Emulator.

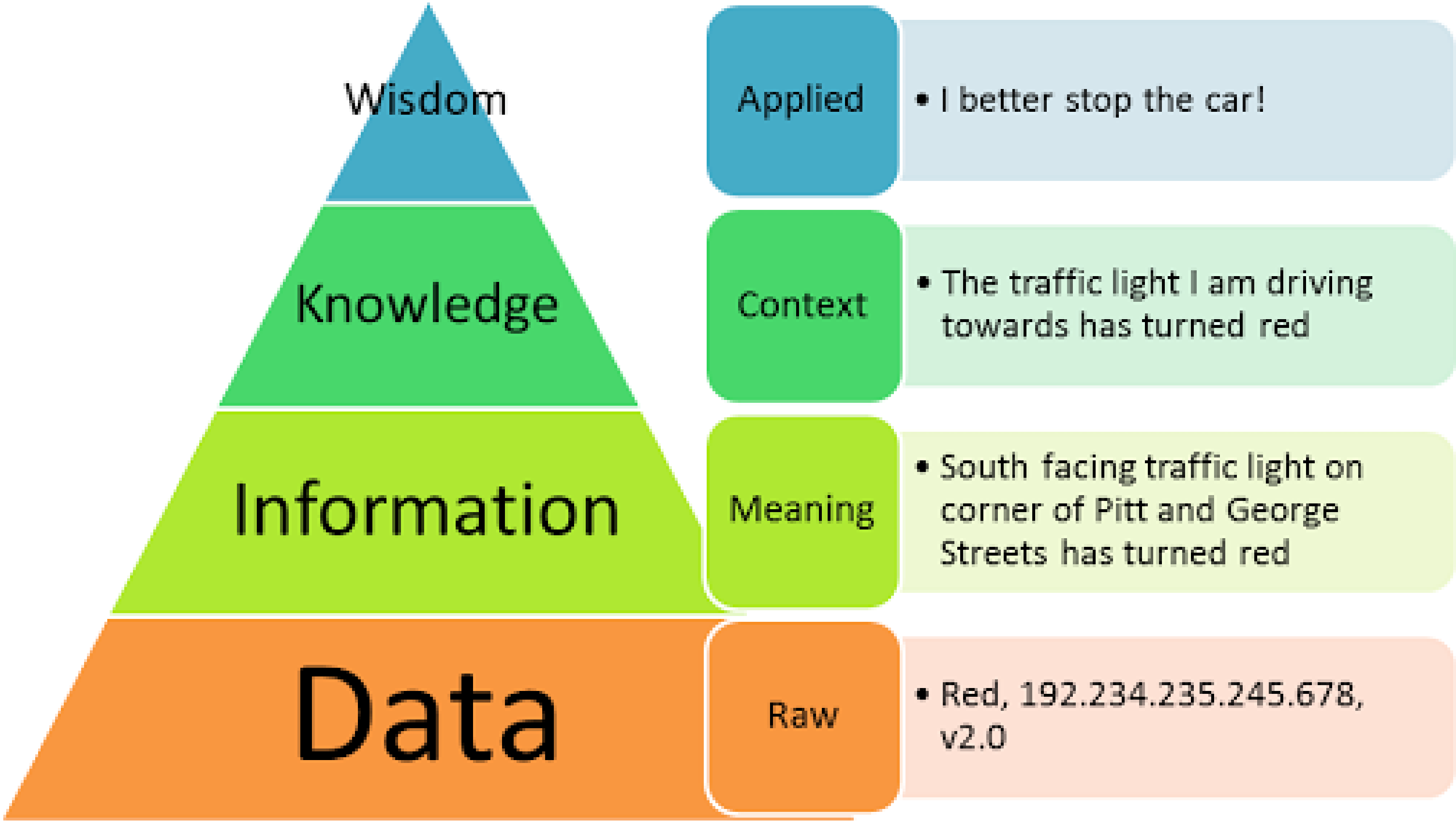
The Hue Emulator is a hue Bridge AP
System.
It allows developers who don't have a
Light Bulbs) to write hue apps.

Hue Emulator

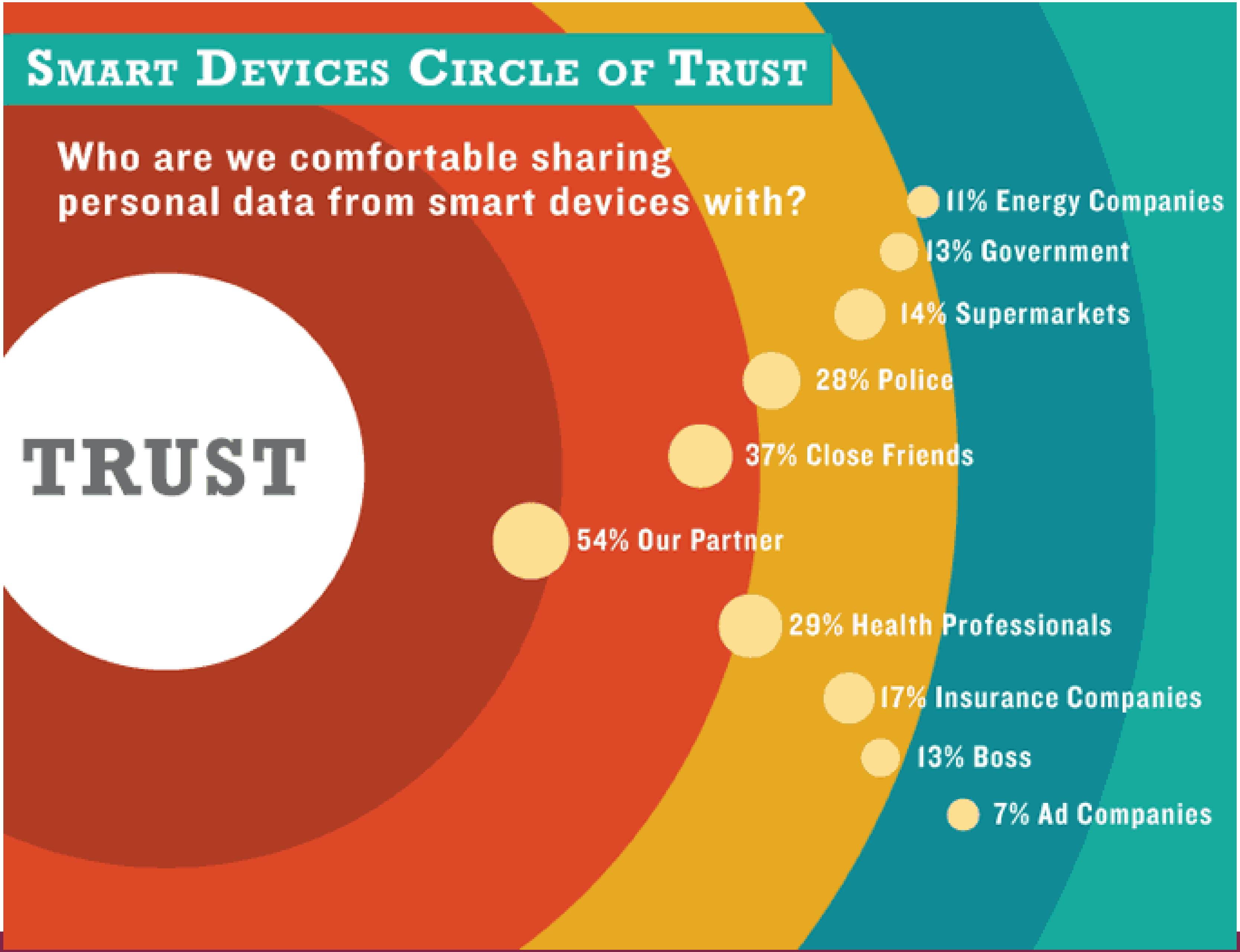
```
Mon, 12 Sep 2016 18:37:10  Loading configuration...
Mon, 12 Sep 2016 18:37:11  Starting Emulator...
Mon, 12 Sep 2016 18:37:11  Welcome to the Hue Emulator.  Choose a port and click the Start Button
```

```
ent/group_(
ercent/grou
lacklistUpd
 --gpu-driv
0b8 --gpu-d
ed-by-fd --
student   3
to chrome
student@ip-
Desktop
student@ip-
student@ip-
SteveyO-Hu
student@ip-
student@ip-
gz
student@ip-
Desktop  De
student@ip-
student@ip-
Desktop  De
student@ip-
student@ip-172-31-20-178:~/hue-emulator$ java -jar HueEmulator-v0.7.jar
▯
```

1
2
3
4
5
6
7
8
9
*
0
A



Wisdom	Applied	• I better stop the car!
Knowledge	Context	• The traffic light I am driving towards has turned red
Information	Meaning	• South facing traffic light on corner of Pitt and George Streets has turned red
Data	Raw	• Red, 192.234.235.245.678, v2.0



Smart Devices Circle of Trust

Who are we comfortable sharing personal data from smart devices with?

TRUST

11% Energy Companies

13% Government

14% Supermarkets

28% Police

37% Close Friends

54% Our Partner

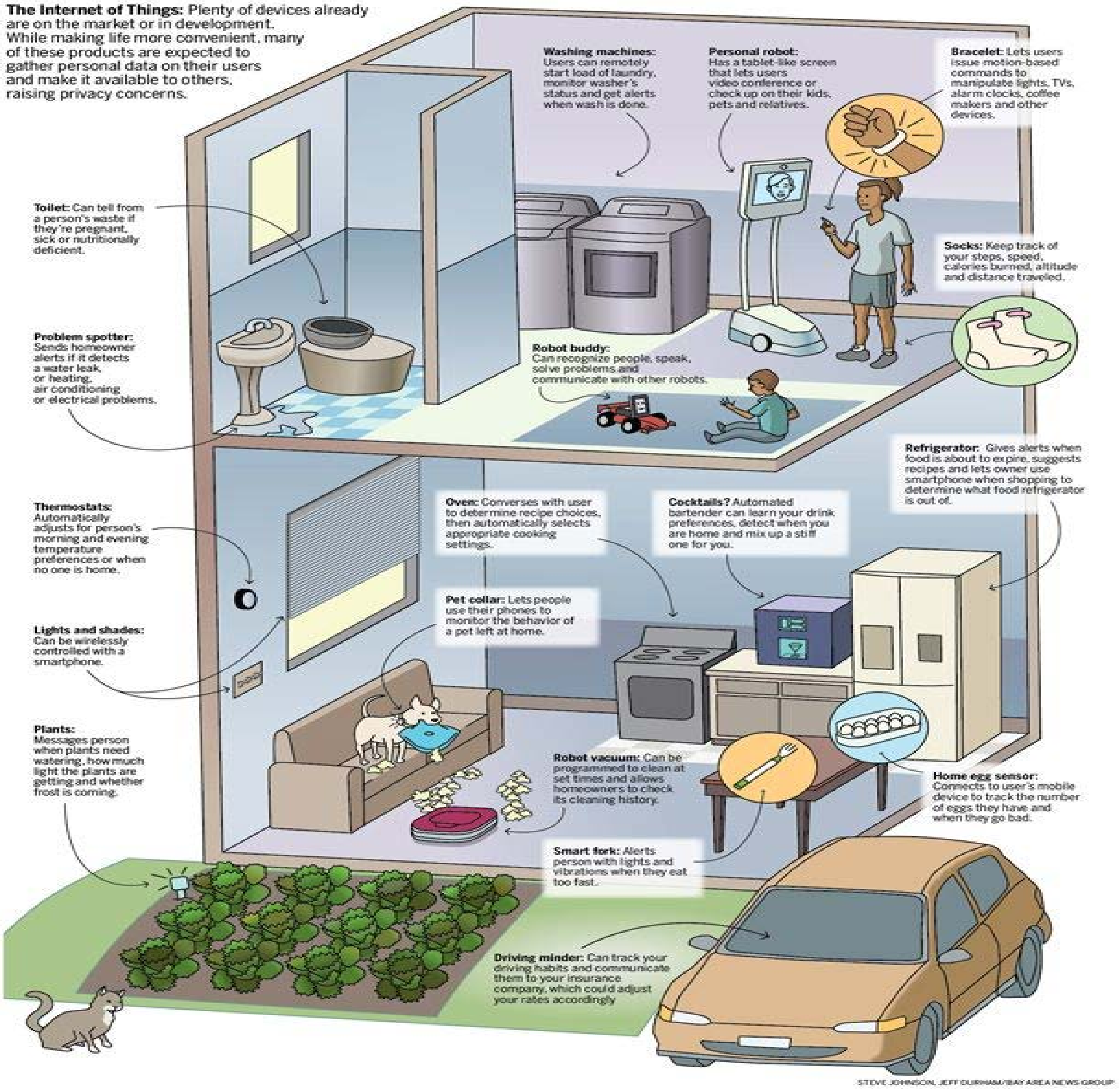
29% Health Professionals

17% Insurance Companies

13% Boss

7% Ad Companies

A world filled with smart gadgets



The Internet of Things: Plenty of devices already are on the market or in development. While making life more convenient, many of these products are expected to gather personal data on their users and make it available to others, raising privacy concerns.

Washing machines: Users can remotely start load of laundry, monitor washer's status and get alerts when wash is done.

Personal robot: Has a tablet-like screen that lets users video conference or check up on their kids, pets and relatives.

Bracelet: Lets users issue motion-based commands to manipulate lights, TVs, alarm clocks, coffee makers and other devices.

Toilet: Can tell from a person's waste if they're pregnant, sick or nutritionally deficient.

Socks: Keep track of your steps, speed, calories burned, altitude and distance traveled.

Problem spotter: Sends homeowner alerts if it detects a water leak, or heating, air conditioning or electrical problems.

Robot buddy: Can recognize people, speak, solve problems and communicate with other robots.

Refrigerator: Gives alerts when food is about to expire, suggests recipes and lets owner use smartphone when shopping to determine what food refrigerator is out of.

Thermostats: Automatically adjusts for person's morning and evening temperature preferences or when no one is home.

Oven: Converses with user to determine recipe choices, then automatically selects appropriate cooking settings.

Cocktails? Automated bartender can learn your drink preferences, detect when you are home and mix up a stiff one for you.

Pet collar: Lets people use their phones to monitor the behavior of a pet left at home.

Lights and shades: Can be wirelessly controlled with a smartphone.

Plants: Messages person when plants need watering, how much light the plants are getting and whether frost is coming.

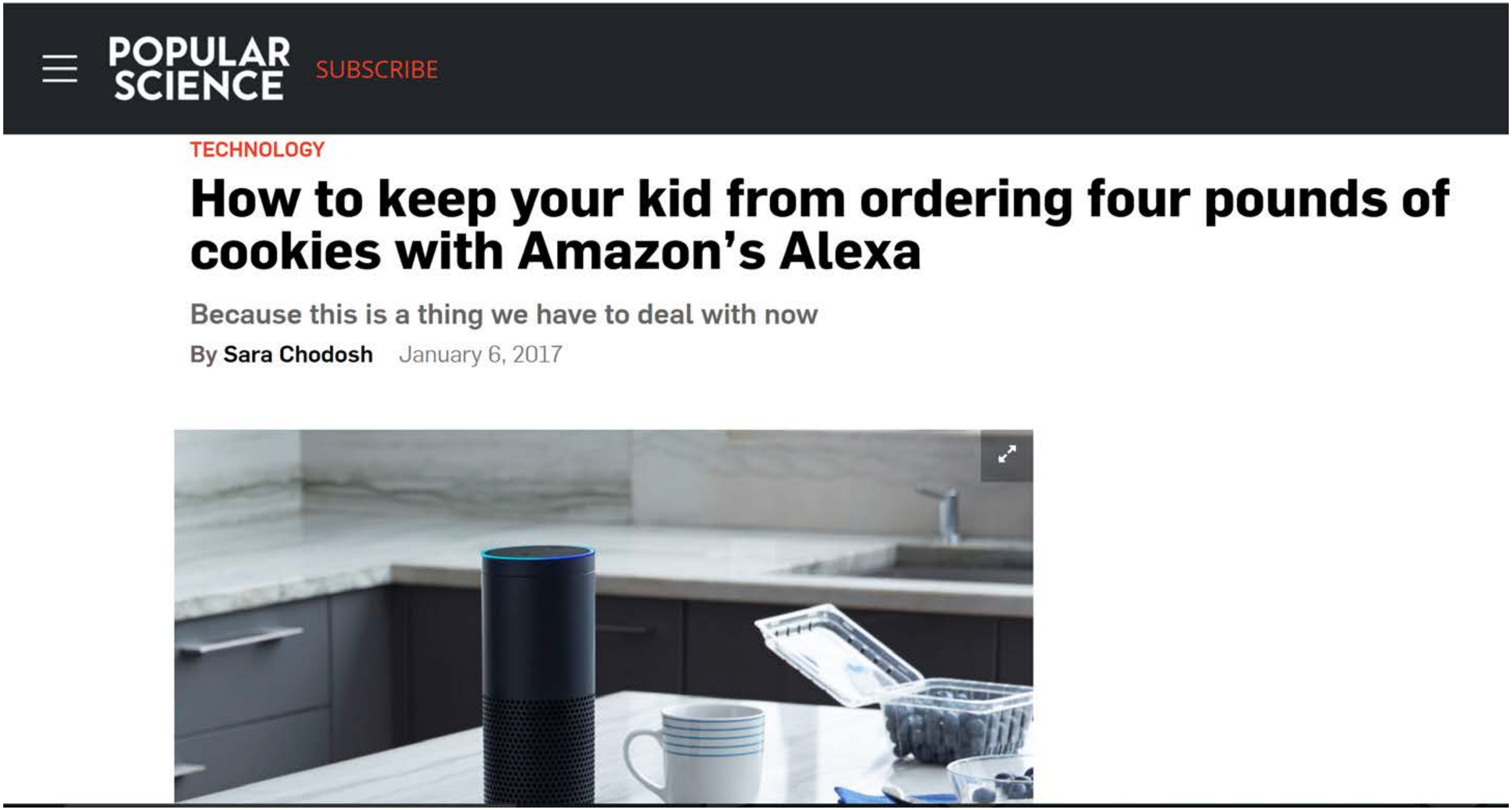
Robot vacuum: Can be programmed to clean at set times and allows homeowners to check its cleaning history.

Home egg sensor: Connects to user's mobile device to track the number of eggs they have and when they go bad.

Smart fork: Alerts person with lights and vibrations when they eat too fast.

Driving minder: Can track your driving habits and communicate them to your insurance company, which could adjust your rates accordingly

STEVE JOHNSON, JEFF DURHAM/BAY AREA NEWS GROUP



POPULAR SCIENCE

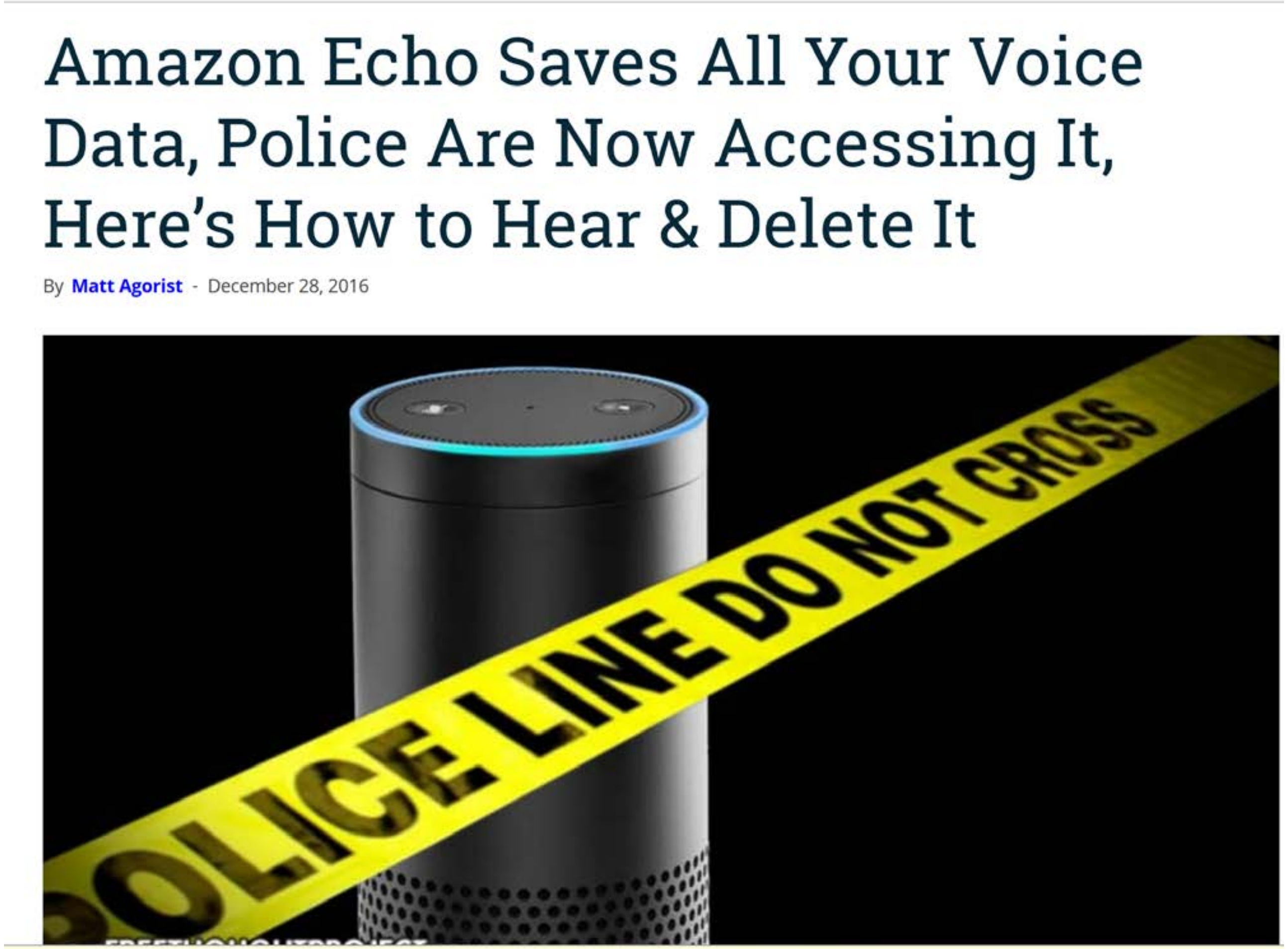
SUBSCRIBE

TECHNOLOGY

How to keep your kid from ordering four pounds of cookies with Amazon's Alexa

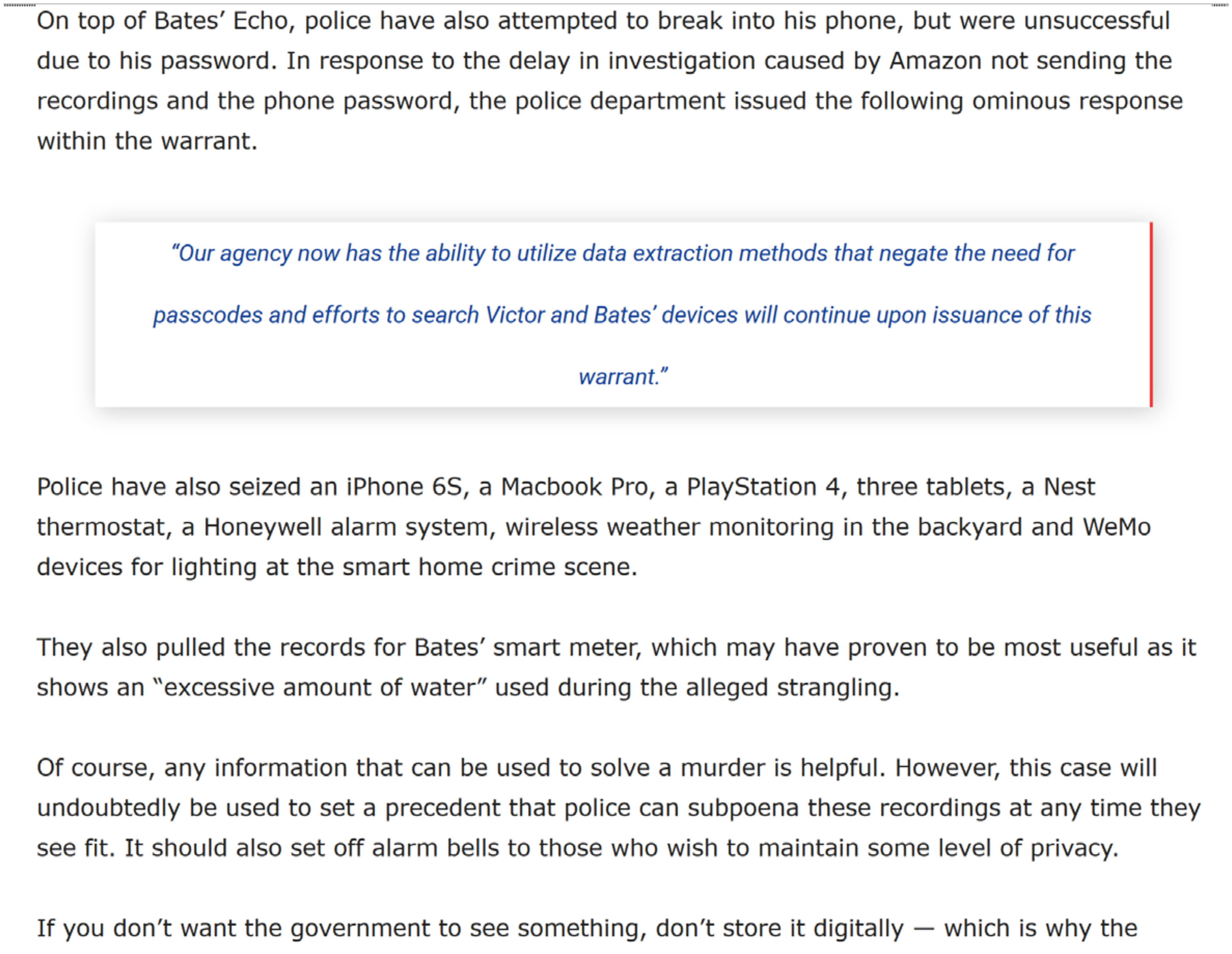
Because this is a thing we have to deal with now

By Sara Chodosh January 6, 2017



Amazon Echo Saves All Your Voice Data, Police Are Now Accessing It, Here’s How to Hear & Delete It

By **Matt Agorist** - December 28, 2016



On top of Bates' Echo, police have also attempted to break into his phone, but were unsuccessful due to his password. In response to the delay in investigation caused by Amazon not sending the recordings and the phone password, the police department issued the following ominous response within the warrant.

> *"Our agency now has the ability to utilize data extraction methods that negate the need for passcodes and efforts to search Victor and Bates' devices will continue upon issuance of this warrant."*

Police have also seized an iPhone 6S, a Macbook Pro, a PlayStation 4, three tablets, a Nest thermostat, a Honeywell alarm system, wireless weather monitoring in the backyard and WeMo devices for lighting at the smart home crime scene.

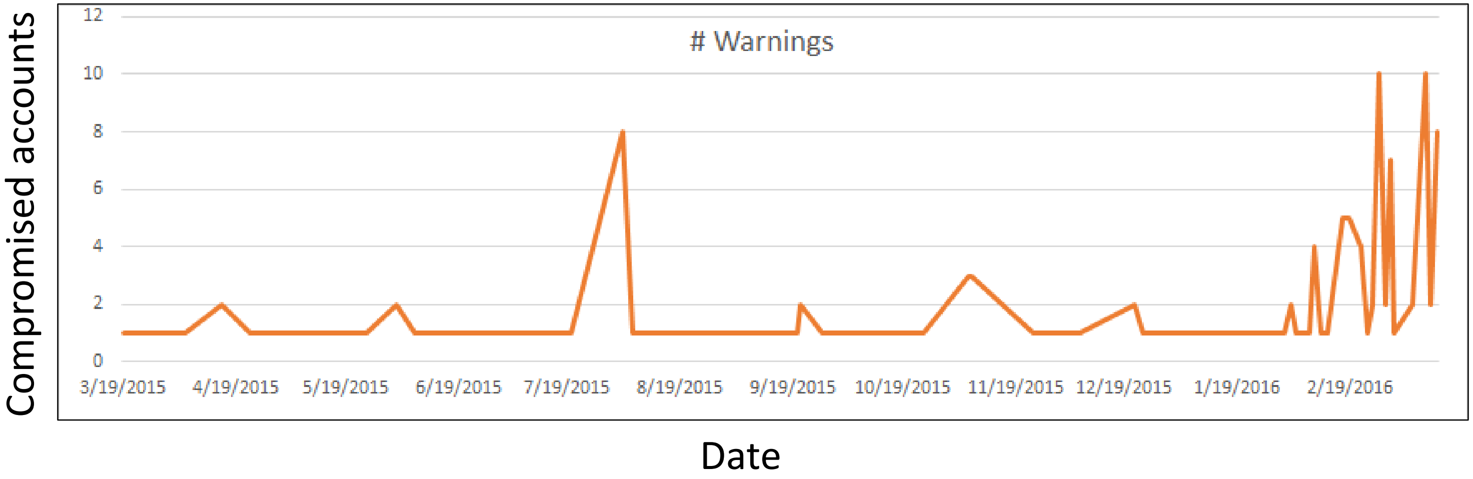
They also pulled the records for Bates' smart meter, which may have proven to be most useful as it shows an "excessive amount of water" used during the alleged strangling.

Of course, any information that can be used to solve a murder is helpful. However, this case will undoubtedly be used to set a precedent that police can subpoena these recordings at any time they see fit. It should also set off alarm bells to those who wish to maintain some level of privacy.

If you don't want the government to see something, don't store it digitally — which is why the

Gmail Account Compromises

- We took action in Jan/Feb to reduce system compromises leading to email spam attacks
- Attackers have changed tactics as we have made their job difficult
- Latest trend is compromised Gmail accounts
  - Fortunately this doesn't help them with spam, but *it can harm individuals whose accounts are compromised!*



Meet a Spammer

March 03, 2016

Direct deposits rerouted after Illinois State University data breach

Share this article:

An attacker compromised the accounts of 13 Illinois State University (ISU) employees and diverted their direct-deposit payroll payments to another account.
The university was alerted of the breach Monday and later learned the attacker rerouted the payments by accessing the victims' university login information, ISU Chief of Staff Jay Groves told *The Pantagraph*.

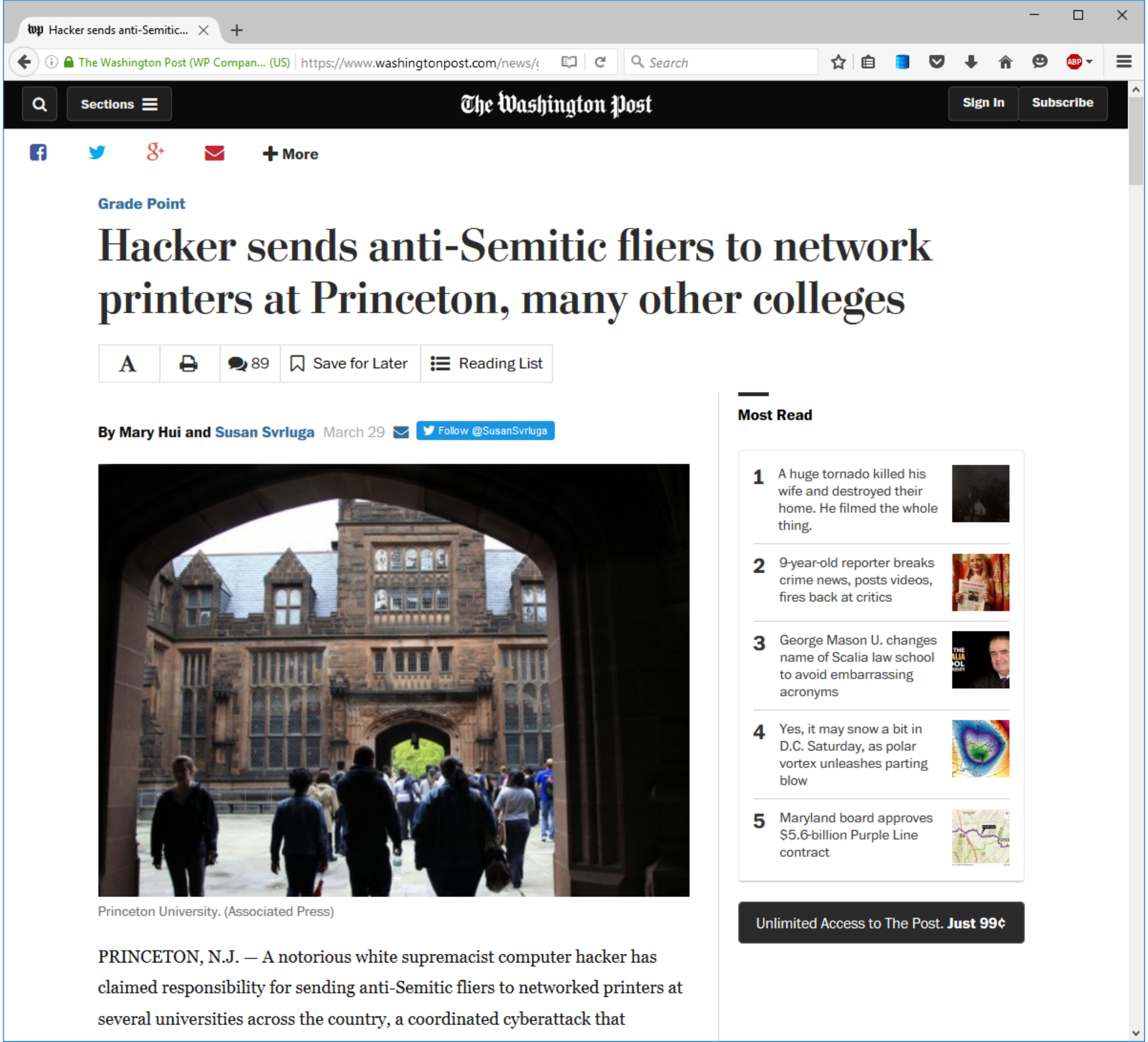
An attacker compromised the payment information of Illinois State University employees.

Those affected have since had the proper amounts credited to their accounts and in order to protect the integrity of other accounts the university has temporarily suspended the ability to modify bank routing information for direct deposits online.

A total of $50,000 was involved in the incident and the university is working with the Federal Bureau of Investigation and Illinois State Police in its investigation.

Faculty, staff and students have been instructed to check their accounts for fraudulent activity.

Groves said there have been five other universities around the country where similar incidents have occurred.


Hacker sends anti-Semitic...
The Washington Post (WP Compan... (US)
https://www.washingtonpost.com/news/(
Search
Sections
Sign In
Subscribe
More
89
Save for Later
Reading List

The Washington Post

Grade Point

Hacker sends anti-Semitic fliers to network printers at Princeton, many other colleges

By Mary Hui and Susan Svrluga March 29 Follow @SusanSvrluga

Princeton University. (Associated Press)

PRINCETON, N.J. — A notorious white supremacist computer hacker has claimed responsibility for sending anti-Semitic fliers to networked printers at several universities across the country, a coordinated cyberattack that

Most Read

1 A huge tornado killed his wife and destroyed their home. He filmed the whole thing.

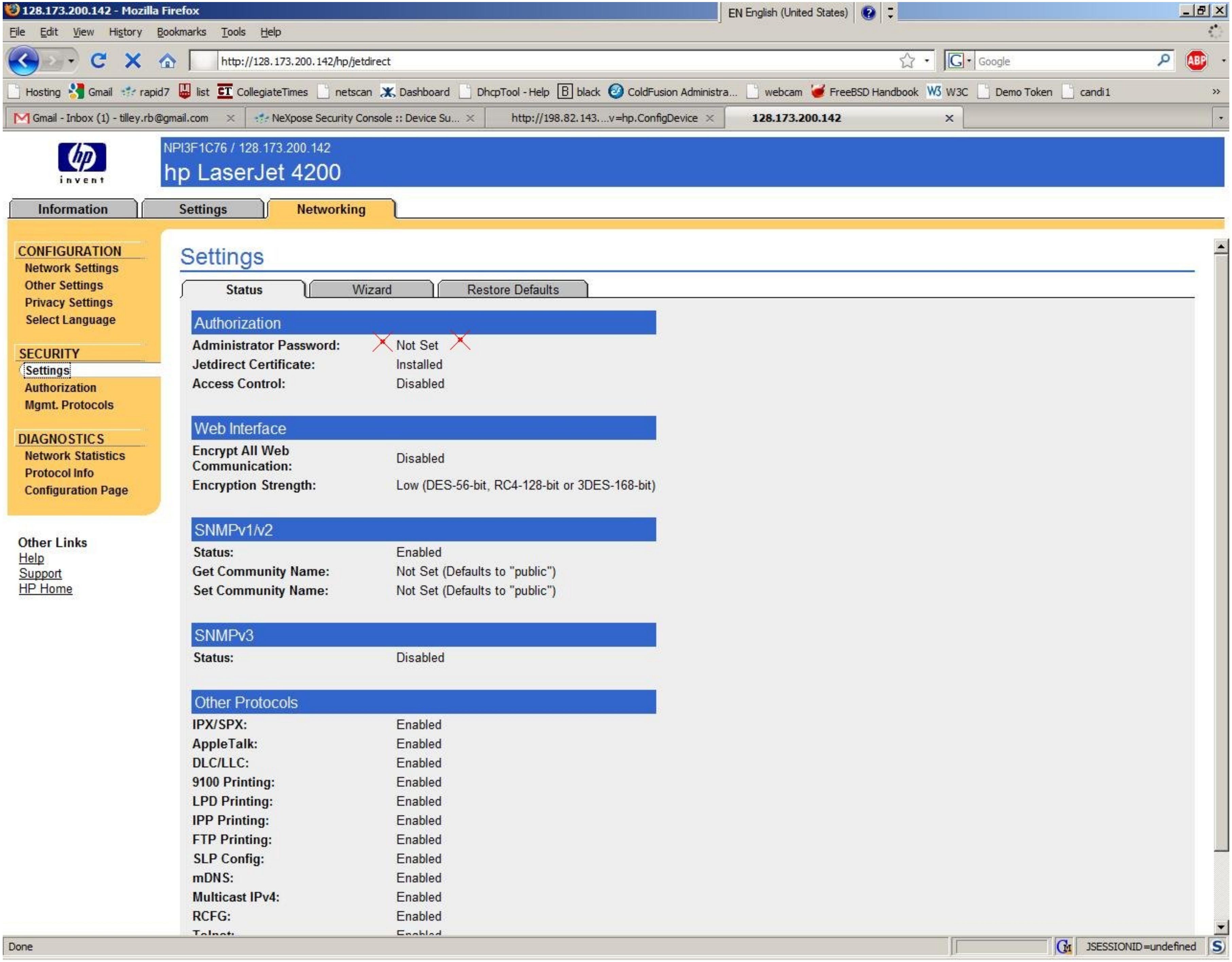
2 9-year-old reporter breaks crime news, posts videos, fires back at critics

3 George Mason U. changes name of Scalia law school to avoid embarrassing acronyms

4 Yes, it may snow a bit in D.C. Saturday, as polar vortex unleashes parting blow

5 Maryland board approves $5.6-billion Purple Line contract

Unlimited Access to The Post. **Just 99¢**



NPI3F1C76 / 128.173.200.142

hp LaserJet 4200

Settings

Authorization

Administrator Password:	Not Set
Jetdirect Certificate:	Installed
Access Control:	Disabled

Web Interface

Encrypt All Web Communication:	Disabled
Encryption Strength:	Low (DES-56-bit, RC4-128-bit or 3DES-168-bit)

SNMPv1/v2

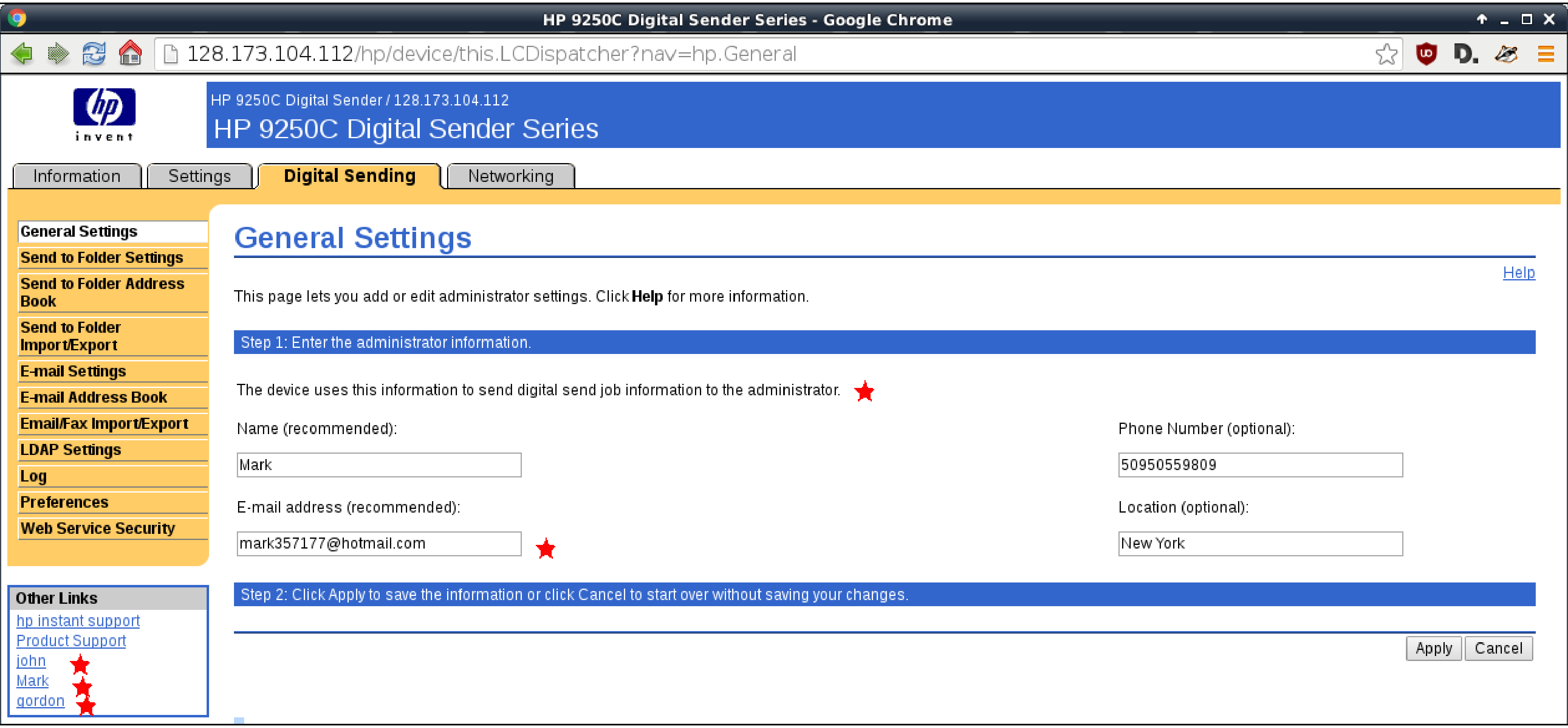
Status:	Enabled
Get Community Name:	Not Set (Defaults to "public")
Set Community Name:	Not Set (Defaults to "public")

SNMPv3

Status:	Disabled

Other Protocols

IPX/SPX:	Enabled
AppleTalk:	Enabled
DLC/LLC:	Enabled
9100 Printing:	Enabled
LPD Printing:	Enabled
IPP Printing:	Enabled
FTP Printing:	Enabled
SLP Config:	Enabled
mDNS:	Enabled
Multicast IPv4:	Enabled
RCFG:	Enabled
Telnet:	Enabled



HP 9250C Digital Sender / 128.173.104.112

HP 9250C Digital Sender Series

General Settings

This page lets you add or edit administrator settings. Click **Help** for more information.

Step 1: Enter the administrator information.

The device uses this information to send digital send job information to the administrator. ★

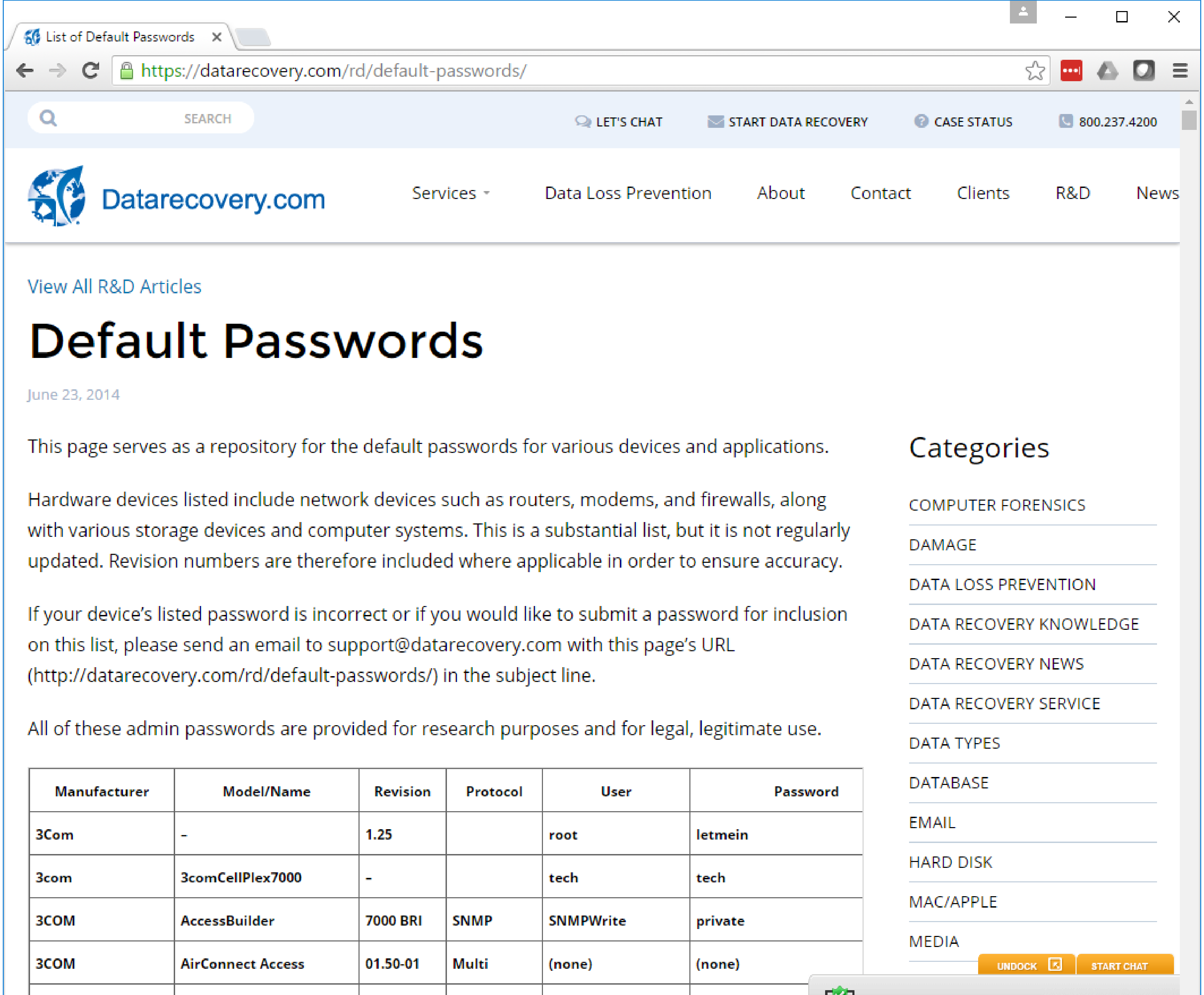
Name (recommended): Mark

Phone Number (optional): 50950559809

E-mail address (recommended): mark357177@hotmail.com ★

Location (optional): New York

Step 2: Click Apply to save the information or click Cancel to start over without saving your changes.



View All R&D Articles

Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

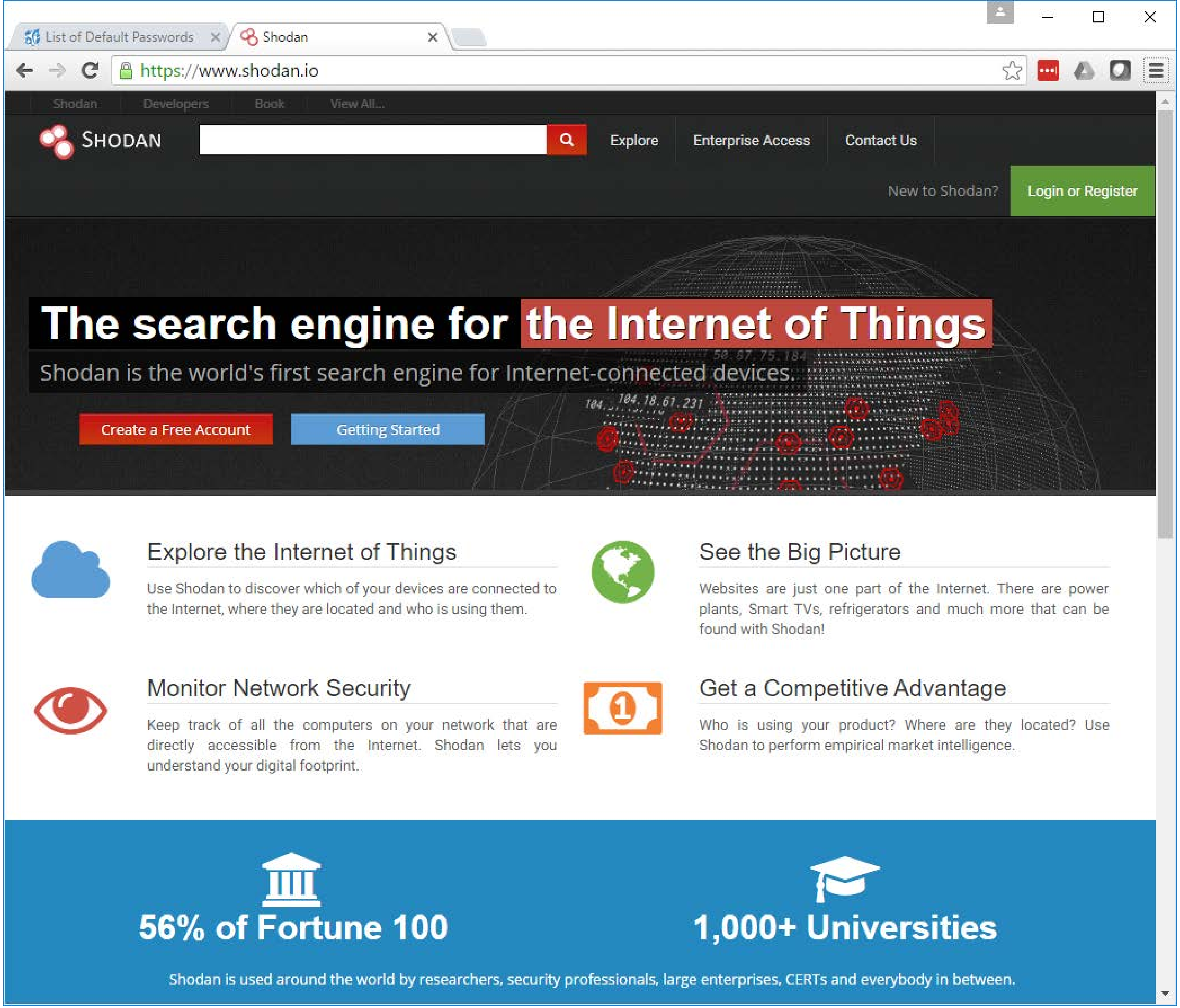
If your device's listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page's URL (http://datarecovery.com/rd/default-passwords/) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

Manufacturer	Model/Name	Revision	Protocol	User	Password
3Com	–	1.25		root	letmein
3com	3comCellPlex7000	–		tech	tech
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite	private
3COM	AirConnect Access	01.50-01	Multi	(none)	(none)

Categories

- COMPUTER FORENSICS
- DAMAGE
- DATA LOSS PREVENTION
- DATA RECOVERY KNOWLEDGE
- DATA RECOVERY NEWS
- DATA RECOVERY SERVICE
- DATA TYPES
- DATABASE
- EMAIL
- HARD DISK
- MAC/APPLE
- MEDIA



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

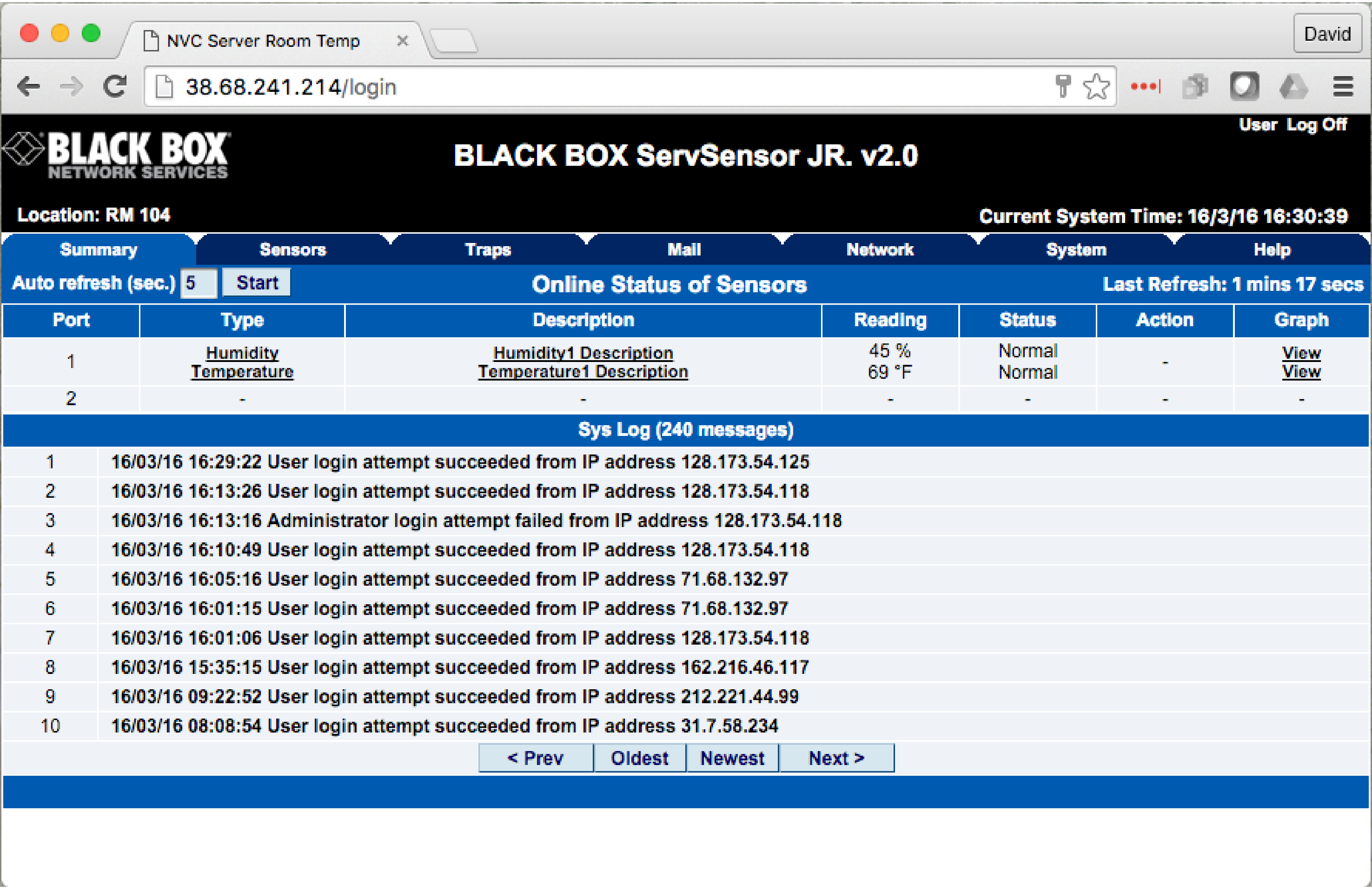
Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.



BLACK BOX ServSensor JR. v2.0

Location: RM 104

Current System Time: 16/3/16 16:30:39

Online Status of Sensors

Last Refresh: 1 mins 17 secs

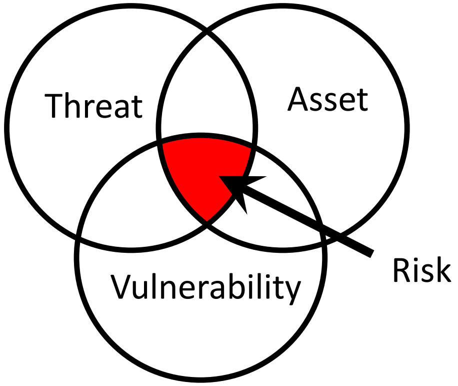
Port	Type	Description	Reading	Status	Action	Graph
1	Humidity Temperature	Humidity1 Description Temperature1 Description	45 % 69 °F	Normal Normal	-	View View
2	-	-	-	-	-	-

Sys Log (240 messages)

```
1   16/03/16 16:29:22 User login attempt succeeded from IP address 128.173.54.125
2   16/03/16 16:13:26 User login attempt succeeded from IP address 128.173.54.118
3   16/03/16 16:13:16 Administrator login attempt failed from IP address 128.173.54.118
4   16/03/16 16:10:49 User login attempt succeeded from IP address 128.173.54.118
5   16/03/16 16:05:16 User login attempt succeeded from IP address 71.68.132.97
6   16/03/16 16:01:15 User login attempt succeeded from IP address 71.68.132.97
7   16/03/16 16:01:06 User login attempt succeeded from IP address 128.173.54.118
8   16/03/16 15:35:15 User login attempt succeeded from IP address 162.216.46.117
9   16/03/16 09:22:52 User login attempt succeeded from IP address 212.221.44.99
10  16/03/16 08:08:54 User login attempt succeeded from IP address 31.7.58.234
```

Consider IoT Risks

- IoT security is negligible
- IoT data collection needs to be understood
- Data Classification becomes important. Be careful with high risk data.
- This is a great place to start as you work to determine your risk exposure

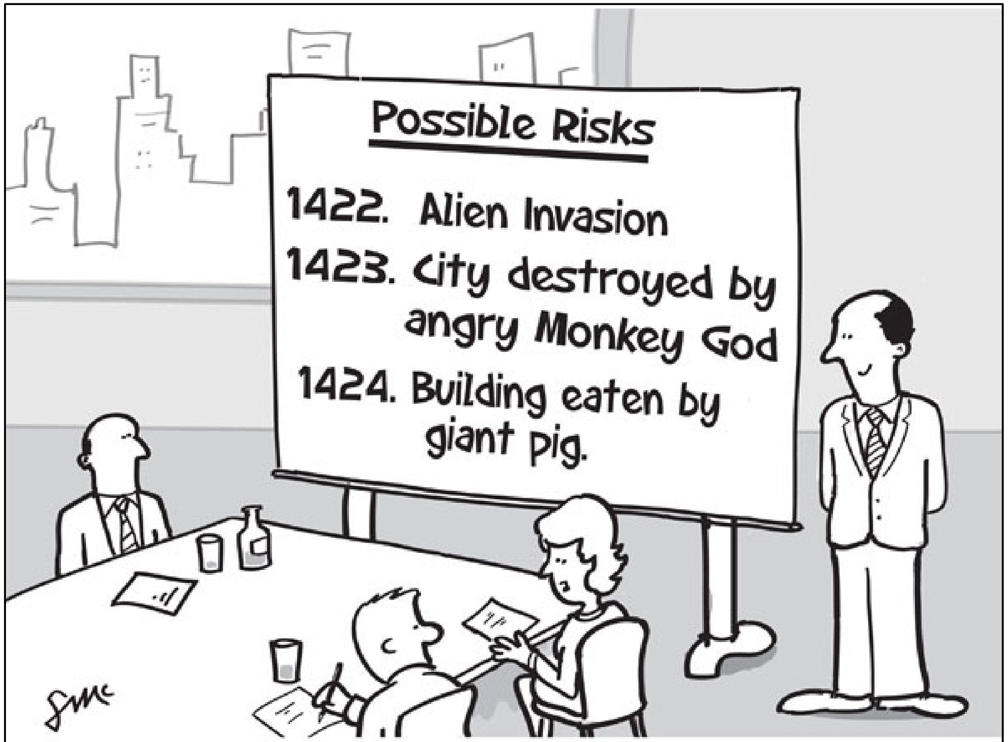


- Asset – something of value to the organization
- Threat – possible danger to asset
- Vulnerability – weakness that leave asset open to threat

Risk = threat X vulnerability

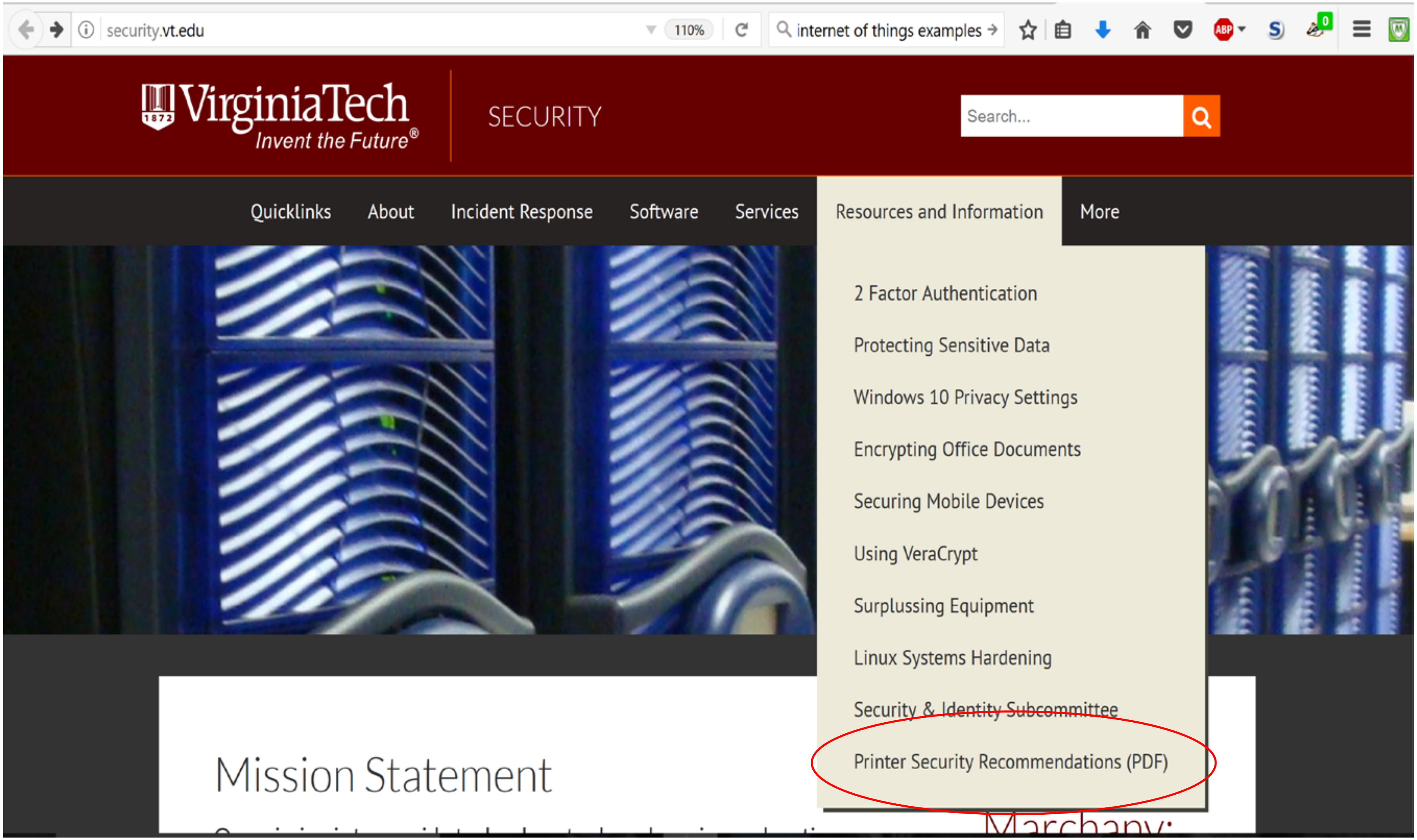
So what do we do?

- Identify assets, prioritize, and address risks
- *You can’t solve everything at once!*


Possible Risks
1422. Alien Invasion
1423. City destroyed by angry Monkey God
1424. Building eaten by giant pig.

“Well he certainly does a very thorough risk analysis.”

Cartoon courtesy of http://www.hardygroupintl.com/blog/tag/risk-reduction/


security.vt.edu
110%
internet of things examples
VirginiaTech
Invent the Future®
SECURITY
Search...
Quicklinks
About
Incident Response
Software
Services
Resources and Information
More
2 Factor Authentication
Protecting Sensitive Data
Windows 10 Privacy Settings
Encrypting Office Documents
Securing Mobile Devices
Using VeraCrypt
Surplussing Equipment
Linux Systems Hardening
Security & Identity Subcommittee
Printer Security Recommendations (PDF)
Mission Statement
Marchany:

Summary

- IoT is pervasive and here to stay
- IoT collects large amounts of data
- Where is it stored?
- Should it be stored there?
- Is it protected?

Thanks to David Raymond, Stephen Huff for the use of their slides

Contact information

- Randy Marchany, Marchany@vt.edu, 540-231-9523 (direct line), 540-231-1688 (office), Twitter: @randymarchany
- http://security.vt.edu