


# 2016 Judicial Family Institute

CyberSecurity at Work, at Home,  
and on the Road




Bryant J. Baehr

Chief Information Officer – Oregon Judicial Department



“There are those who  
have been hacked and  
realize it and those who  
have been hacked and  
haven’t”

John Hering, Founder of Lookout  
Information Security  
60 Minutes report  
April 17, 2016

A vertical computer monitor and keyboard are visible on the left side of the slide. The monitor is white with a blue border and a small keyboard area at the bottom. The keyboard is white with blue accents. The mouse is white and positioned in front of the keyboard.

Your smartphone is  
technically more powerful  
than the computing power  
used to send the Apollo  
astronauts to the moon and  
back



WOW!

I thought that only my friends  
could read my Facebook  
posts

“Those who say interesting things on  
Facebook and wonder how the media  
found out”



**Geez Grandma! It's not that hard! Go into Settings... select Wi-Fi... Select it! Tap it with your finger... OMG any finger!! Grrrrr**

# What we used to talk about

- Georgia Department of Labor – 1,000 personnel records sent to wrong email address
- Virginia Department of Human Resources – 13,000 personnel records sent to wrong email address
- Medical University of South Carolina – 7,000 personnel records compromised
- Missouri Dental Office – 10,000 patient records compromised
- Adobe – 38 million user ID's and passwords compromised

# What we used to talk about

Oregon Secretary of State – business/elections database hacked. February 2014

Oregon Department of Employment – 851,300 records compromised. October 2014

Maricopa Community College (MCC) – 2 million records compromised – April 2013 – cost \$26,000,000.00 so far



What a difference two  
(2) years make...







70 million individuals (partial name, mailing address, phone, email) 40 million credit / debit card

56 million credit / debit cards



78.8 million individuals (SS#'s, DOB, addresses, medical ID's)



76 million individuals (name, address, phone #, email)

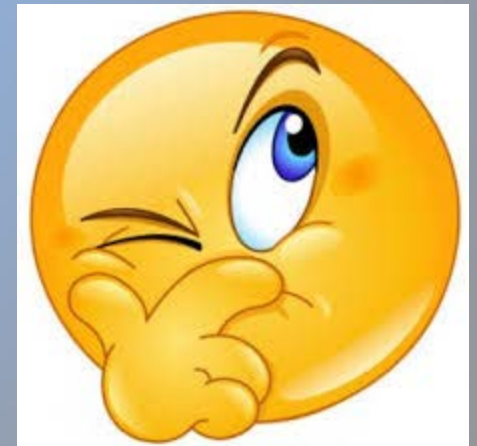


Approximately 395 stores impacted



My life is not that exciting -  
why target me?

Actually, you are exciting  
to hackers and those who  
want to disrupt your life.



# What is the CyberSecurity landscape today?

https://stopthinkconnect.org/

File Edit View Favorites Tools Help

STOP | THINK | CONNECT

Partner Resource Center | About | Contact

Keeping the web a safer place for everyone.

Home Tips & Advice Campaigns Resources Research & Surveys Blog Get Involved

**President Obama Supports New STOP. THINK. CONNECT. Efforts Industry commits to collaborate on online safety and security**

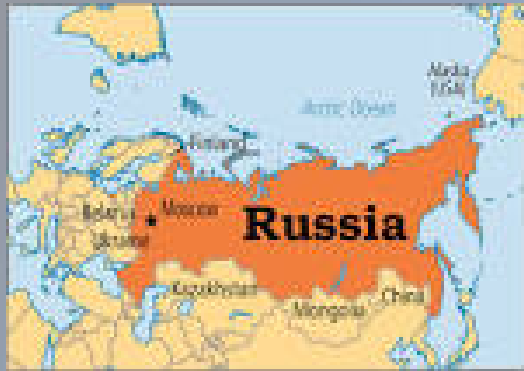
Learn More

**Tips & Advice**

- Basic Tips & Advice (English)
- Basic Tips & Advice (Spanish)
- Safety Tips for Mobile Devices
- Basic Tips & Advice (French (Canadian))

**Did You Know?**

96% of Americans feel a personal responsibility to be safer and more secure online



## Nation States – National Crime Rings




Data aggregators, Phone scammers, Your neighbor



# Identity Theft:

Identity compromised – credit / purchasing impact  
Government impact – travel, taxes  
On-line impact – Facebook, Twitter, social media



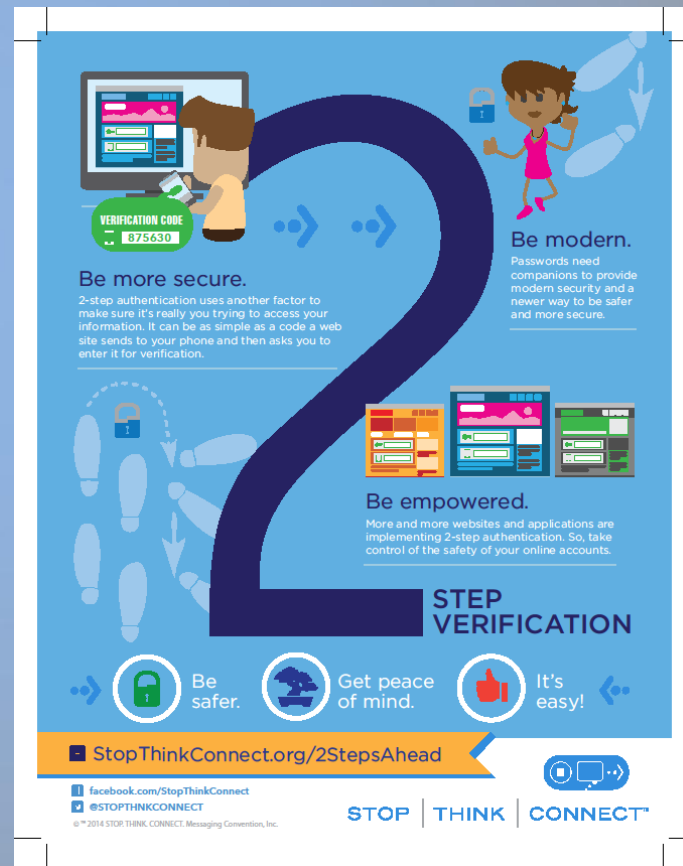
STOP | THINK | CONNECT™

**I OWN MY ONLINE PRESENCE!**

By controlling my internet security and privacy settings, I can share only what I'm comfortable sharing.

[www.stopthinkconnect.org](http://www.stopthinkconnect.org)

CYBER SECURITY



**Be more secure.**  
2-step authentication uses another factor to make sure it's really you trying to access your information. It can be as simple as a code a web site sends to your phone and then asks you to enter it for verification.

**Be modern.**  
Passwords need companions to provide modern security and a newer way to be safer and more secure.

**Be empowered.**  
More and more websites and applications are implementing 2-step authentication. So, take control of the safety of your online accounts.

**STEP VERIFICATION**

Be safer. Get peace of mind. It's easy!

StopThinkConnect.org/2StepsAhead

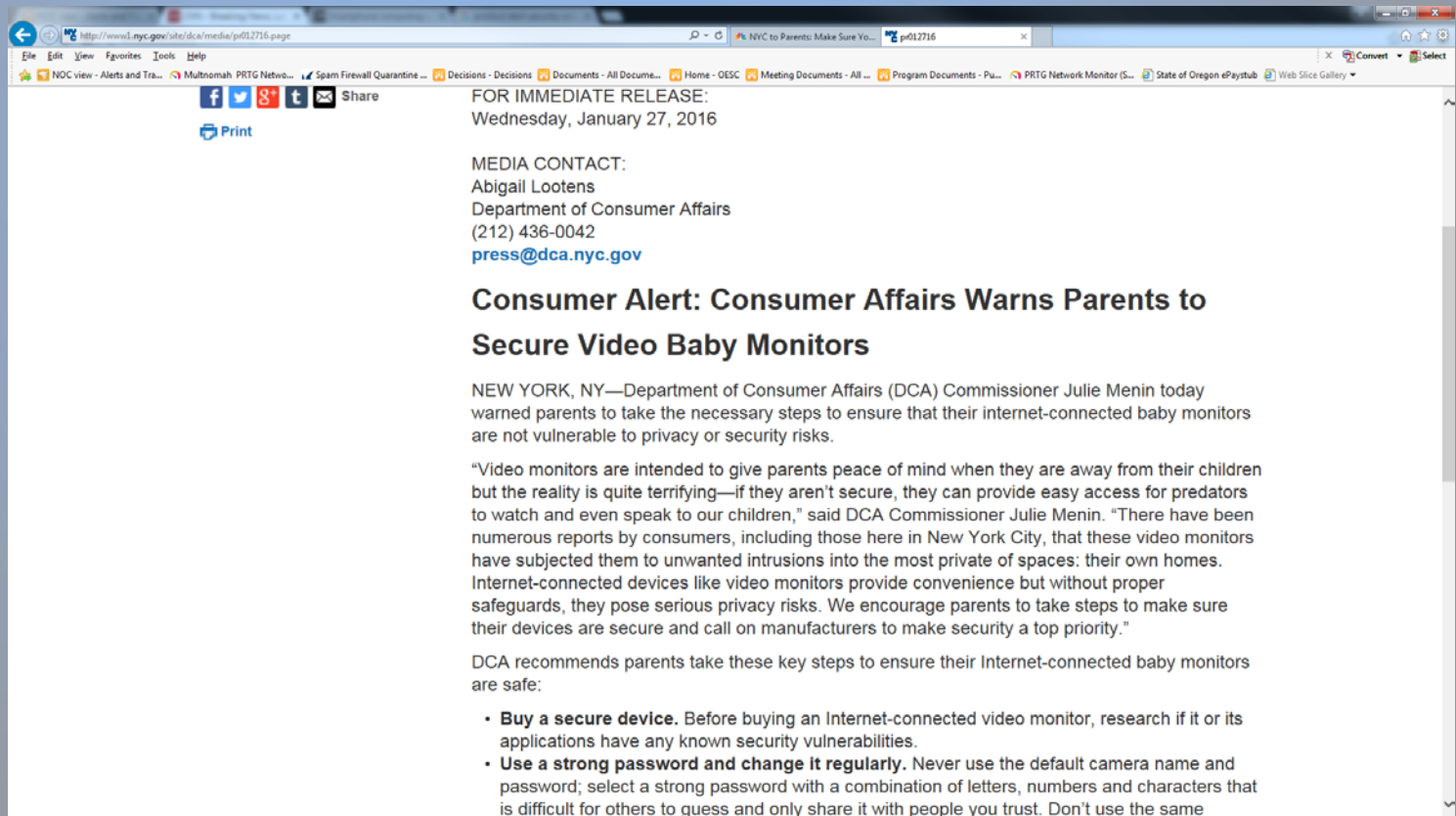
facebook.com/StopThinkConnect  
@STOPTHINKCONNECT

STOP | THINK | CONNECT™

© 2014 STOP THINK, CONNECT, Messaging Convention, Inc.

# Home Wi-Fi hacked:

- Network traffic from others flows through your system
- Access to your computers and anything attached to your WiFi system are compromised
- Camera / Alarm systems are compromised



The screenshot shows a web browser window with the URL <http://www1.nyc.gov/site/dca/medial/pr012716.page>. The page content includes a "FOR IMMEDIATE RELEASE" notice dated Wednesday, January 27, 2016, and a "Consumer Alert: Consumer Affairs Warns Parents to Secure Video Baby Monitors". The alert text states that the Department of Consumer Affairs (DCA) Commissioner Julie Menin has warned parents to take necessary steps to ensure their internet-connected baby monitors are not vulnerable to privacy or security risks. It also provides a list of key steps for parents to take.

**FOR IMMEDIATE RELEASE:**  
Wednesday, January 27, 2016

**MEDIA CONTACT:**  
Abigail Lootens  
Department of Consumer Affairs  
(212) 436-0042  
[press@dca.nyc.gov](mailto:press@dca.nyc.gov)

**Consumer Alert: Consumer Affairs Warns Parents to Secure Video Baby Monitors**

NEW YORK, NY—Department of Consumer Affairs (DCA) Commissioner Julie Menin today warned parents to take the necessary steps to ensure that their internet-connected baby monitors are not vulnerable to privacy or security risks.

"Video monitors are intended to give parents peace of mind when they are away from their children but the reality is quite terrifying—if they aren't secure, they can provide easy access for predators to watch and even speak to our children," said DCA Commissioner Julie Menin. "There have been numerous reports by consumers, including those here in New York City, that these video monitors have subjected them to unwanted intrusions into the most private of spaces: their own homes. Internet-connected devices like video monitors provide convenience but without proper safeguards, they pose serious privacy risks. We encourage parents to take steps to make sure their devices are secure and call on manufacturers to make security a top priority."

DCA recommends parents take these key steps to ensure their Internet-connected baby monitors are safe:

- **Buy a secure device.** Before buying an Internet-connected video monitor, research if it or its applications have any known security vulnerabilities.
- **Use a strong password and change it regularly.** Never use the default camera name and password; select a strong password with a combination of letters, numbers and characters that is difficult for others to guess and only share it with people you trust. Don't use the same

# Malware downloaded to your personal computer or phone:

Copy all data/pictures

Monitor/copy email – send email as you

Access credit card information in other applications

Activate camera without your knowledge

The screenshot shows a web browser displaying the Federal Trade Commission's website. The page is titled "CONSUMER INFORMATION" and features a sidebar with navigation links such as "MONEY & CREDIT", "HOMES & MORTGAGES", "HEALTH & FITNESS", "JOBS & MAKING MONEY", "PRIVACY & IDENTITY", "BLOG", "VIDEO & MEDIA", and "SCAM ALERTS". The main content area is titled "Tech Support Scams" and includes a search bar, a "View this page in español" link, and a "Related Items" section with a video thumbnail titled "Protect Your Computer from Malware". The text on the page describes how scammers use phone calls to trick users into giving them remote access to their computers, often claiming to be from well-known companies like Microsoft. It also provides links to "How Tech Support Scams Work", "If You Get a Call", "If You've Responded to a Scam", and "How to Spot a Refund Scam".

FEDERAL TRADE COMMISSION

CONSUMER INFORMATION

Search

View this page in español

### Tech Support Scams

In a recent twist, scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies like Microsoft. They say that they've detected viruses or other malware on your computer to trick you into giving them remote access or paying for software you don't need.

These scammers take advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard time and again that it's important to install security software. But the purpose behind their elaborate scheme isn't to protect your computer, it's to make money.

- How Tech Support Scams Work
- If You Get a Call
- If You've Responded to a Scam
- How to Spot a Refund Scam

### How Tech Support Scams Work

Scammers have been peddling bogus security software for years. They set up fake websites, offer free "security" scans, and send alarming messages to try to convince you that your computer is infected. Then, they try to sell you software to fix the problem. At best, the software is worthless or available elsewhere for free. At worst, it could be malware — software designed to give criminals access to your computer and your personal information.

The latest version of the scam begins with a phone call. Scammers can get your name and other basic information from public directories. They might even guess what computer software you're using.

Once they have you on the phone, they often try to gain your trust by pretending to be associated with well-known companies or confusing you with a barrage of technical terms. They may ask you to go to your computer and perform a series of complex tasks. Sometimes, they target legitimate computer files and claim that they are viruses. Their tactics are designed to scare you into believing they can help fix your "problem."

Once they've gained your trust, they may:

- Malware
- Phishing



# Cyber Exploitation:

The non-consensual distribution or publication of intimate photos or videos online.

NOC view - Alerts and Tr... Judge declares 'Cyberst... Cyberstalker Sentenced to...  
https://www.justice.gov/opa/pr/cyberstalker-sentenced-10-years-prison

en ESPAÑOL

HOME ABOUT AGENCIES BUSINESS RESOURCES NEWS CAREERS CONTACT

Home » Office of Public Affairs » Briefing Room » Justice News

**JUSTICE NEWS**

Department of Justice  
Office of Public Affairs

FOR IMMEDIATE RELEASE Tuesday, March 1, 2016

**Cyberstalker Sentenced to 10 Years in Prison**

Michael Daniel Rubens, 31, formerly of Tallahassee, Florida, was sentenced today to 10 years in prison, a \$15,000 fine and \$1,550 in restitution for cyberstalking, unauthorized access to a protected computer and aggravated identity theft. The sentence was announced by Acting U.S. Attorney Christopher P. Canova for the Northern District of Florida.

During his guilty plea on Dec. 3, 2015, Rubens admitted that, between January 2012 and January 2015, he publicly humiliated dozens of young women by hacking into their online accounts, including e-mail and social media, stealing photographs and other personal information, using the photographs to create pornography and posting the pornographic images on social media websites and on a revenge pornography website that was recently shut down by the FBI. Rubens engaged in most of the conduct from his residence in Tallahassee. He used software to conceal his IP address.

Rubens' victims included an employee of a local restaurant he frequented, an out-of-town colleague, an acquaintance in his office building, clients of the defendant's employer, a former girlfriend and her colleagues, high school classmates and the victims' relatives or friends. For one particular woman, Rubens' laptop contained 470 files with more than 5,000 references to the victim. Rubens' computer searches focused on finding the victims' personal identifying information, such as past addresses, family information and other personal data that could be used to answer security questions. As a result of Rubens' conduct, the victims became afraid to conduct any online activities and often deleted their social media presence

DEPARTMENT OF JUSTICE ACCOMPLISHMENTS

OPEN GOVERNMENT AT THE DEPARTMENT OF JUSTICE

SMART ON CRIME

DEPARTMENT OF JUSTICE ACTION CENTER  
Report a Crime

# Using technology to attempt to gain a specific result

- Instances of fake websites,
- Instagram – LSU Discussion
- FaceBook, Twitter



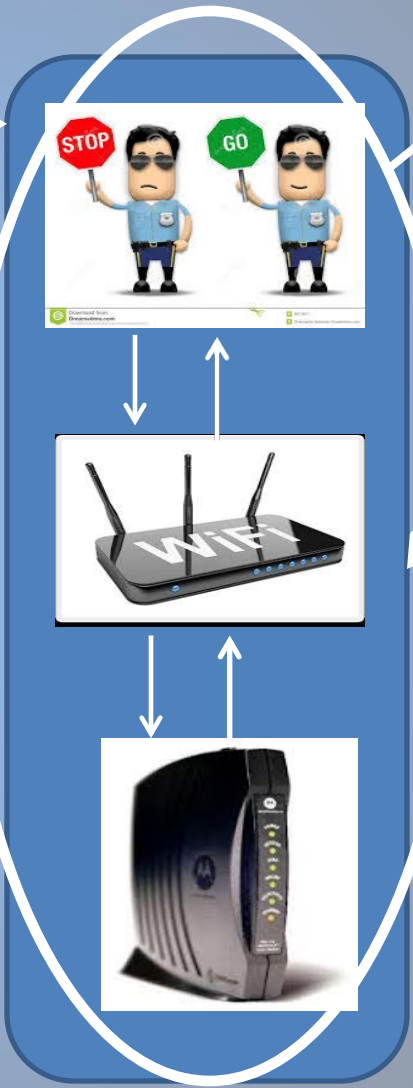
Zanie Kasem – 25 yrs old

- 
- Fraudulent use of an email account
  - Becoming Facebook friends with family member in an effort to influence outcome
  - Cracking cloud service accounts to gain access to photos/information



# What can we do?

# CyberSecurity - Home



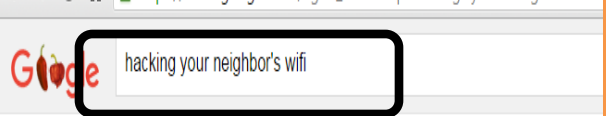
Firewall & Password





Firewall & Password





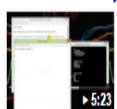
All News Videos Images Shopping More Search tools  
About 13,800 results (0.29 seconds)

### How to hack your neighbors WiFi for free WORKS - YouTube



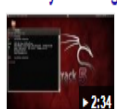
https://www.youtube.com/watch?v=iDvGnwsHmPI  
Dec 23, 2013 - Uploaded by kom76live  
2 easy steps if you dont get caught you get free internet !!!!

### How to find any wifi password of your neighbor ... - YouTube



https://www.youtube.com/watch?v=erHRfJlbSI  
Dec 25, 2014 - Uploaded by Tech & IT  
Today i will show you how to find your connected wifi password with CMD? ... Guys I'm using a great tool ...

### Hack your Neighbour wi-fi in 10 mins - YouTube



https://www.youtube.com/watch?v=Mv9yy1u3VUI  
Jan 13, 2013 - Uploaded by Cyber Shield  
even if your Neighbors are smart enough to use wpa2, still u can crack it in 10 min. use it for testing/education ...

### How to Steal Your Neighbors Wifi - YouTube



https://www.youtube.com/watch?v=yWhU\_eTYIYY  
Aug 8, 2014 - Uploaded by ThioJoe  
Highly requested tutorial on how to steal your neighbors wifi so you can use it for yourself!! No hacking ...

### How To Hack Neighbor's WI FI It Works - YouTube

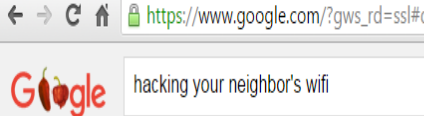


https://www.youtube.com/watch?v=nLkq9gDOFQ  
Sep 28, 2011 - Uploaded by Terence Ogarte  
How To Hack Neighbor's WI FI It Works .... How to find any wifi password of your neighbor wifi password or ...

### how to hack your neighbors internet - YouTube



https://www.youtube.com/watch?v=mwF79vfBhMA  
Oct 10, 2009 - Uploaded by thecomputerhowtodo  
I just hacked my wife facebook. its free make sure you follow the steps ... How to scare your neighbors: Name ...



All News Videos Images Shopping More Search tools  
About 164,000 results (0.47 seconds)

### How to Crack Wi-Fi Passwords—For Beginners! « Hacks ...

modsn-hacks.wonderhowto.com/.../crack-wi-fi-passwords-for-beginners...  
Oct 16, 2012 - Cracking those Wi-Fi passwords is your answer to temporary internet access. ... How to Hack WiFi Passwords for Free Wireless Internet on Your PS3 ..... Want to take advantage of your neighbor's super fast Wi-Fi connection? How to Hack WPA WiFi ... - How to Hack Wi-Fi: Cracking ...

### How to Hack Wi-Fi Passwords | PCMag.com

www.pcmag.com > ... > Software > Security > Networking > PC Magazine >  
Mar 6, 2015 - Perhaps you forgot the password on your own network, or don't have neighbors willing to share the Wi-Fi goodness. You could just go to a café ...

### How to hack your neighbors WiFi for free WORKS - YouTube



https://www.youtube.com/watch?v=iDvGnwsHmPI  
Dec 23, 2013 - Uploaded by kom76live  
2 easy steps if you dont get caught you get free internet !!!!

### 5 Ways To Hack Into Your Neighbor's Wifi Network - Tips4pc

tips4pc.com > Computer tips and tricks >  
Nov 9, 2014 - Hacking into your neighbor's wifi network may be easier than you think —and, conversely, your neighbor may think it's easy to hack into your ...

### How to steal Wifi - wifi password hacking - Step to step

comorobarwifi.org/how-to-steal-wifi >  
As the title says, with this tutorial we will know how to steal wifi from your neighbour. ... To hack neighbors wifi, I mean to check the security of our network, we are ...

### How I cracked my neighbor's WiFi password without ...

arstechnica.com/security/.../wireless-password-easily-crack... > Ars Technica >  
Aug 28, 2012 - How I cracked my neighbor's WiFi password without breaking a sweat .... It's also true that it's trivial for hackers in your vicinity to capture the ...

### How to hack a Wi-Fi network - Quora

https://www.quora.com/How-can-I-hack-a-Wi-Fi-network-1 Quora >  
This is a catchall question for Wi-Fi hacking, including password bypass or password You may not be creating a security gap, but your repairman servicemen When I

# Password Complexity


beachboys	2 minutes
thebeachboys	4 weeks
theb3achboys	4 years

---

theb#achboys	18 years
--------------	----------

th#B3achB)Y%	- 47,000,000 years
--------------	--------------------





# CyberSecurity – Why would someone want to access my WiFi?

- Turn off your alarm system
- Gain access to your house
- Access your computers – data
- Control appliances – lights – temperature - TV
- Use your network to do bad things (steal services)

# What can we do?

- Change factory WiFi password to complex password Th#B3achB)Y% (TheBeachBoys)
- Establish a “guest” network – even if your family members live with you (allow them to share with trusted friends)



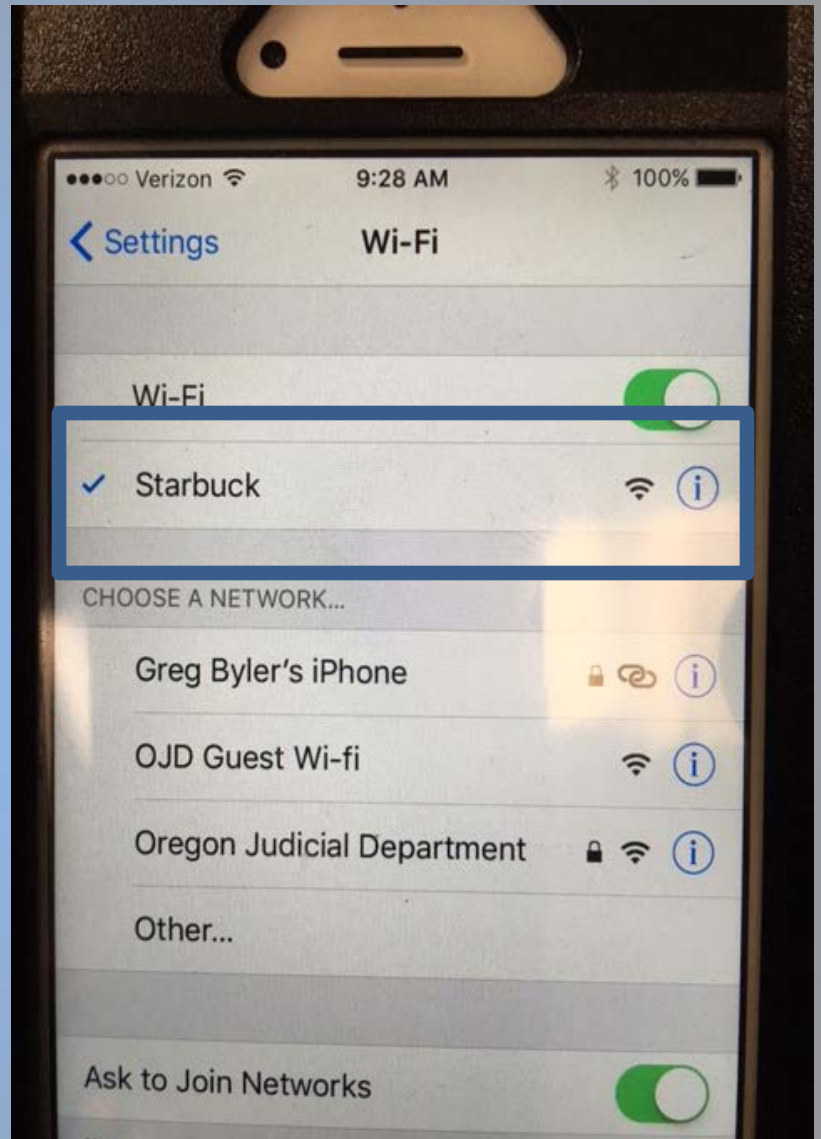
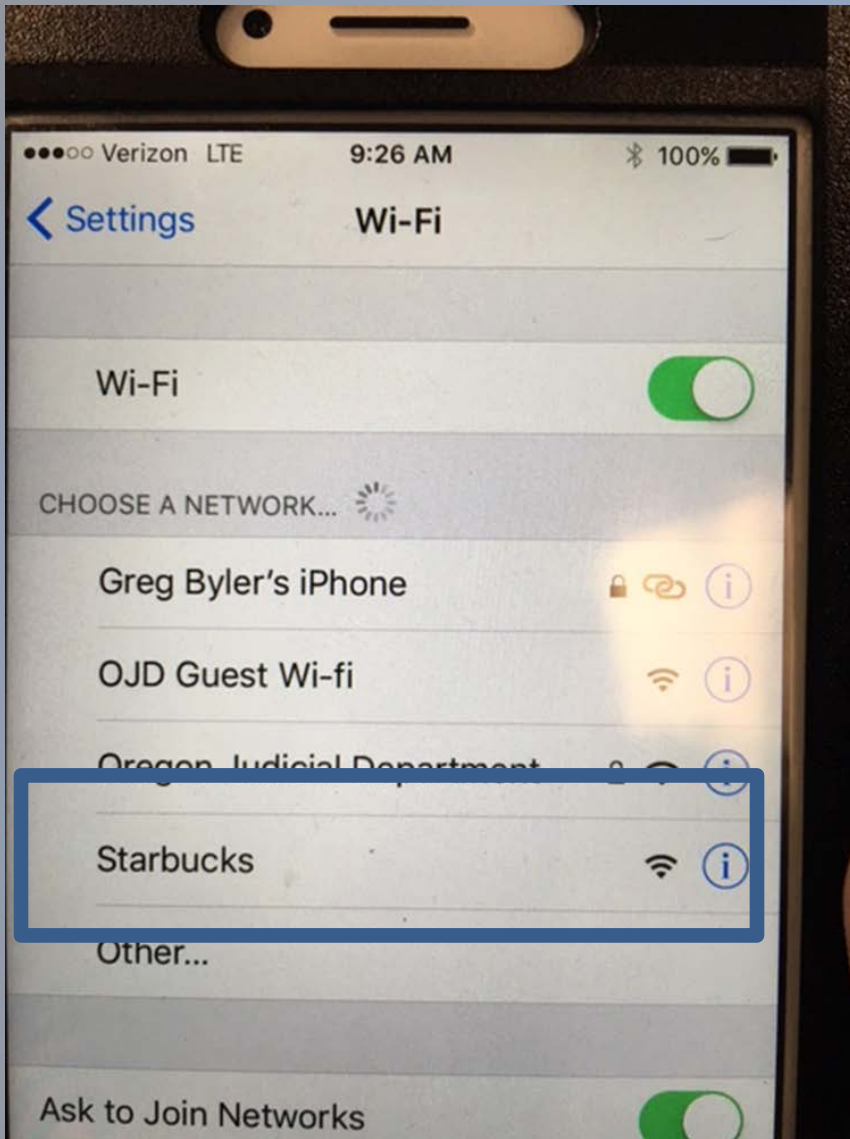
# What can we do?

- Rarely let “apps” store your password
- If you have a wireless camera system, have a separate password for that application/system
- Never name your WiFi “Baehr Family Network”



# CyberSecurity – Away from Home

- Be careful when using “free” WiFi or “tethering”
- Never store personal information “SS# - DOB” on your mobile device
- Use credit card versus debit card
- Link smaller savings account versus large savings account to debit card



# CyberSecurity – Away from Home

- Always have a password/passcode on mobile device
- If you are going to use the “cloud” to store items, use major company: Apple, Microsoft, Amazon versus smaller vendor or “free” vendor
- I generally do not “tag” my pictures with location / date / time information
- Turn on “find my iPhone” “Android Device Manager” service



# CyberSecurity – Away from Home



**WITHOUT**



**WITH**

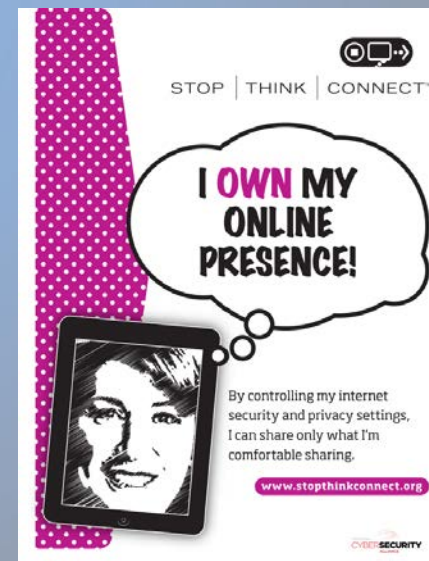




# CyberSecurity – Facebook

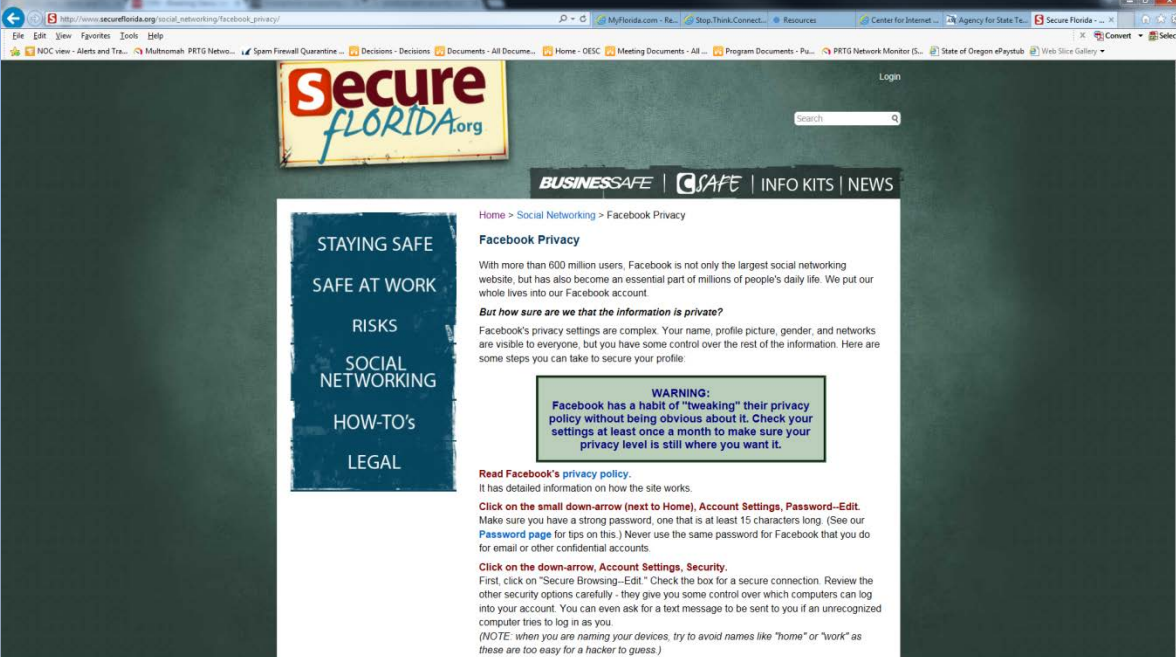
- Be selective with your “friends”
- Enact privacy settings – don’t “tag” pictures with date/time
- Log-out when not using
- Limit PII information (such as high school attended, year graduated, where you work, cars you drive)

You may be the target so a specific outcome can be achieved



# CyberSecurity – Facebook

- Complex password
- Know that “Facebook stalking” is real and it could be one of your “friends” accounts that is compromised
- Announce when you have returned – not when leaving for vacation



The screenshot shows a web browser window displaying the Secure Florida website. The URL in the address bar is [http://www.secureflorida.org/social\\_networking/facebook\\_privacy/](http://www.secureflorida.org/social_networking/facebook_privacy/). The page features the Secure Florida logo at the top left and a navigation menu with links for BUSINESSSAFE, SAFE, INFO KITS, and NEWS. A sidebar on the left lists categories: STAYING SAFE, SAFE AT WORK, RISKS, SOCIAL NETWORKING, HOW-TO's, and LEGAL. The main content area is titled "Facebook Privacy" and includes the following text:

Home > Social Networking > Facebook Privacy

### Facebook Privacy

With more than 600 million users, Facebook is not only the largest social networking website, but has also become an essential part of millions of people's daily life. We put our whole lives into our Facebook account.

**But how sure are we that the information is private?**

Facebook's privacy settings are complex. Your name, profile picture, gender, and networks are visible to everyone, but you have some control over the rest of the information. Here are some steps you can take to secure your profile.

**WARNING:**  
Facebook has a habit of "tweaking" their privacy policy without being obvious about it. Check your settings at least once a month to make sure your privacy level is still where you want it.

**Read Facebook's privacy policy.**  
It has detailed information on how the site works.

**Click on the small down-arrow (next to Home), Account Settings, Password-Edit.**  
Make sure you have a strong password, one that is at least 15 characters long. (See our Password page for tips on this.) Never use the same password for Facebook that you do for email or other confidential accounts.

**Click on the down-arrow, Account Settings, Security.**  
First, click on "Secure Browsing-Edit." Check the box for a secure connection. Review the other security options carefully - they give you some control over which computers can log into your account. You can even ask for a text message to be sent to you if an unrecognized computer tries to log in as you.  
(NOTE: when you are naming your devices, try to avoid names like "home" or "work" as these are too easy for a hacker to guess.)

# CyberSecurity – Computer

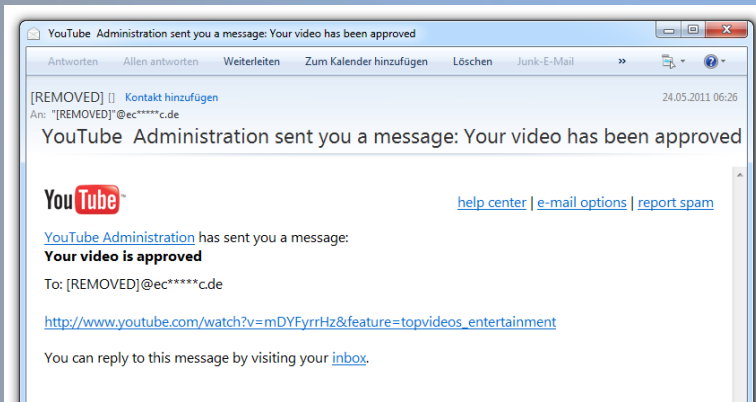
Latest anti-virus – look for status icon

Firewall settings – generally go with factory recommendations

Do not allow someone to take over your computer that calls you or sends you a “pop-up” request!

# CyberSecurity – email

- Never click on a link
- Never open a file
- Always go to a specific location



From: [uec\\_100@hotmail.com](mailto:uec_100@hotmail.com)  
To: [noreply@hotmail.com](mailto:noreply@hotmail.com)  
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)  
Date: Sun, 1 Feb 2015 23:15:37 +0530



Dear Email User,

This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support and security. If you choose not to update your account on or before **4th February, 2015**, you will read and send emails, and you will no longer have access to many of the latest features for improved conversations, contacts and attachments.

[Update Your Account](#)

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.

**Thank You**  
**Outlook Warning! Member Service**

**Walmart** 

Save money. Live better.

[Electronics](#) [Movies](#) [Home](#) [Baby](#) [Toys](#) [Video games](#) [Photo](#)

This letter is to advise you about the order we have which is addressed to you. You have 4 days to pick it in any Local Store of Walmart.

Please, follow this [link](#) for more information about your order.

Walmart is wishing you Happy Thanksgiving Day!

[Store Finder](#) [Local AD](#) [Returns & Exchanges](#) [Privacy & Security](#)

Copyright (c) 2014 WalMart | All rights reserved

**From:** Facebook [<mailto:notification@facebook.com>]  
**Sent:** 17 July 2012 15:38  
**To:**   
**Subject:** Christine McLain Gibbs tagged a photo of you on Facebook

facebook



[Christine McLain Gibbs](#) added a photo of you.

[See Photo](#)

[Go to Notifications](#)

If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).

Facebook, Inc. Attention: Department 415 P.O. Box 10005 Palo Alto CA 94303

## Home - Security

- Talk / engage your Neighbors
- Alarm system – regular maintenance and testing
- Battery backup (router – WiFi)– most systems are reactive, not proactive
- Family communication

# CyberSecurity at Work

Cybersecurity processes and procedures will slow you down a bit

Change password regularly

Report suspicious activity / emails

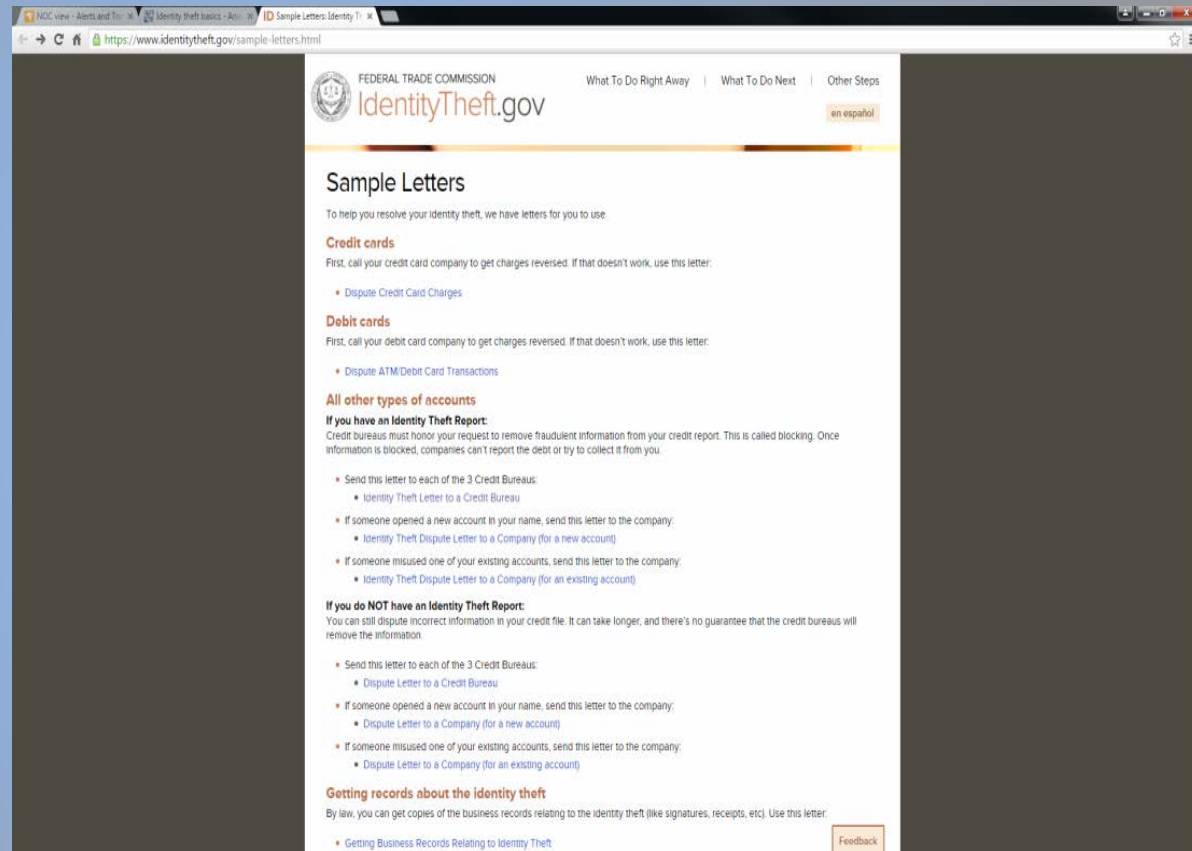
Report suspicious items attached to the network



# Identity Monitoring Tools – Have a Plan!

3 credit rating agencies:

- Equifax
- Experian
- TransUnion

















The screenshot shows the IdentityTheft.gov website. The header includes the Federal Trade Commission logo and the text "IdentityTheft.gov". There are navigation links for "What To Do Right Away", "What To Do Next", and "Other Steps", along with a "en español" button. The main content area is titled "Sample Letters" and provides instructions on how to resolve identity theft. It includes sections for "Credit cards", "Debit cards", and "All other types of accounts". Each section provides a brief explanation and a list of steps to take, such as sending letters to credit bureaus or disputing charges. A "Feedback" button is visible at the bottom right of the page.

Annualcreditreport.com



## CyberSecurity – Recommendations and Tips

	<ul style="list-style-type: none"> <li>• Use complex password (phrase and %&amp;#)</li> <li>• Change name if "Smith Family WiFi"</li> <li>• Activate guest network and use a different password</li> <li>• Router "recommended" WiFi firewall settings are okay to use</li> <li>• Attach battery backup to service provider router</li> </ul>
	<ul style="list-style-type: none"> <li>• Have different password and make it complex</li> <li>• If using cell phone "app" use different password</li> <li>• Do not leave "logged in"</li> </ul>
	<ul style="list-style-type: none"> <li>• Place family members on "guest" network</li> <li>• Allow them to share "that" password with friends as appropriate</li> <li>• Use router recommended firewall settings for guest network to increase security</li> </ul>
	<ul style="list-style-type: none"> <li>• Do not open unsolicited email and/or attachments</li> <li>• If in question, go directly to site versus following in email link</li> <li>• Do not use the contact information in the email, Find and contact directly</li> </ul>
	<ul style="list-style-type: none"> <li>• Just because you can connect it to your WiFi does not mean you should</li> <li>• Question when family members want to connect a device to your network</li> <li>• Remember that connecting friends (or family member friends) to your network means that internet traffic accessed by others will flow through your personal system</li> </ul>
	<ul style="list-style-type: none"> <li>• Lock phone – code/PIN</li> <li>• Turn on "find my iPhone" or "Android Device Manager"</li> <li>• Do not store PII information on phone</li> <li>• Do not "tag" pictures with time/date/location stamp</li> <li>• Do not store password on sensitive applications (web cams)</li> </ul>

	<ul style="list-style-type: none"> <li>• Check for battery backup</li> <li>• Check connection to company (VOIP or POTS)</li> <li>• Regularly check system and panic button</li> <li>• Ensure that family members don't share access code</li> </ul>
	<ul style="list-style-type: none"> <li>• Exterior lights – automatic timers</li> <li>• Companies provide home safe assessments</li> <li>• Keep garage door openers hidden</li> <li>• Have house look "lived in" when gone</li> </ul>
	<ul style="list-style-type: none"> <li>• Enact privacy settings</li> <li>• Careful on who you "friend"</li> <li>• Ask "friends" regarding their privacy</li> <li>• Complex password</li> </ul>
	<ul style="list-style-type: none"> <li>• Watch for "skimmers"</li> <li>• Watch surroundings</li> <li>• Daylight and in an active area is generally the best time to use an ATM machine</li> </ul>
	<ul style="list-style-type: none"> <li>• Check credit reports yearly</li> <li>• If victim of identity theft – have a plan - notify bank, credit cards, credit agencies, freeze credit accounts</li> </ul>
	<ul style="list-style-type: none"> <li>• Updated anti-virus</li> <li>• Firewall settings on computer – generally recommended "okay"</li> <li>• Do not allow someone to "take over" your personal computer</li> </ul>
	<ul style="list-style-type: none"> <li>• Use major company</li> <li>• Ensure that password is "very" complex</li> <li>• Look as to where your information is stored (some store overseas)</li> </ul>
	<ul style="list-style-type: none"> <li>• Only join known networks</li> <li>• Do not join "personal" networks or networks that appear to be spelled funny</li> <li>• Know that your information will be accessible while using a public network. Always look for HTTPS:// - no banking should be done on free Wi-Fi</li> </ul>

Next???



Flagstaff 2017?



## CONTACT INFORMATION:

Bryant J. Baehr  
Chief Information Officer  
Oregon Judicial Department  
1163 State Street  
Salem, Oregon 97301

503-986-4515

[Bryant.Baehr@OJD.STATE.OR.US](mailto:Bryant.Baehr@OJD.STATE.OR.US)