Conference of Chief Justices
*Midyear Meeting – 2016*

CyberSecurity: How to stay safe

Bryant J. Baehr
Chief Information Officer – Oregon Judicial Department
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 were sent to wrong email address
- Medical University of South Carolina – 7,000 personnel records were compromised
- Missouri Dental Office – 10,000 patient records compromised
- Adobe – 38 million user ID’s and passwords
What a difference one (1) year makes...
70 million individuals (partial name, mailing address, phone, email) 40 million credit / debit card accounts

56 million credit / debit cards

78.8 million records (SS#’s, DOB, addresses, medical ID’s)

76 million name, address, phone #, email

Approximately 395 stores impacted
Is there anyone who has not been “hacked?”

The worst is over!

My life is not that exciting, why target me?
Nation States – National Crime Rings

Data aggregators, Phone scammers, *Your neighbor*
Michigan man accused of cyberstalking 10 local females

Many victims are underage girls.

By Phil Fairbanks | News Staff Reporter | @PhilFairbanksIV | Google+
on November 17, 2012 - 11:23 PM

One by one, the young women came to the Kenmore police with disturbing tales of a stranger sending them messages, some by text, some through Facebook and Twitter.

His demands were clear: Communicate with me or I'll send more pictures of you to your friends and family.

Over time, it became clear to investigators that this was no ordinary case of stalking but the work of a savvy individual with a sophisticated knowledge of technology.

The number of victims, meanwhile, started to mount — 10 at last count, all from Western New York and many of them underage girls. Even more alarming, perhaps, the two police suspected behind it all lived more than 300 miles away in Michigan.

“We don’t have geography as a limiting factor anymore,” said Christopher M. Piorko, special agent in charge of the FBI office in Buffalo. “The physical boundaries that were once a factor in stalking? They’ve been removed.”
The victim told detectives that when she asked Kasem to stop contacting her office via phone and email the woman created a public website and posted personal photos of the judge and her family, including three minor children, to it. Kasem also allegedly created an Instagram account and posted photos of the judge and her family there as well. Both the website and the Instagram account had text content that made claims that accused the judge of being a corrupt thief.
CyberSecurity - Home
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 (other apps like controlling your TV, I set to remember)
- Never name your wifi “Baehr Family Network”
CyberSecurity – Away from Home

- Use credit card versus debit card
- Link smaller savings account versus large savings account to debit card
- Be aware that your device is tracking you
- Be careful when using “free” Wifi or “tethering”
- Never store personal information “SS# - DOB” on your mobile device
CyberSecurity – Away from Home

• Always have a password/passcode on mobile device (cell).

• 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 actually real and it could be one of your “friends” accounts that is compromised.
CyberSecurity – Facebook

• Announce when you have returned from vacation not that you are leaving.
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

- Click on a link
- Open a file
- Go to a specific location
Home - Security

Lighten up exterior/interior – use automatic timers

Handheld Garage Door Openers – not in car parked outside

Remove items from clear view (car)
Home - Security

- Neighbors
- Alarm system – regular maintenance and testing
- Battery backup (router – WiFi)– most systems are reactive not proactive
- Family Communication
Home - Security

- Most use phone/internet – you can get cell backup
- Free security assessment
- Communication with family
Identity Monitoring Tools

3 credit rating agencies:
• Equifax
• Experian
• TransUnion

Annualcreditreport.com
Next???
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