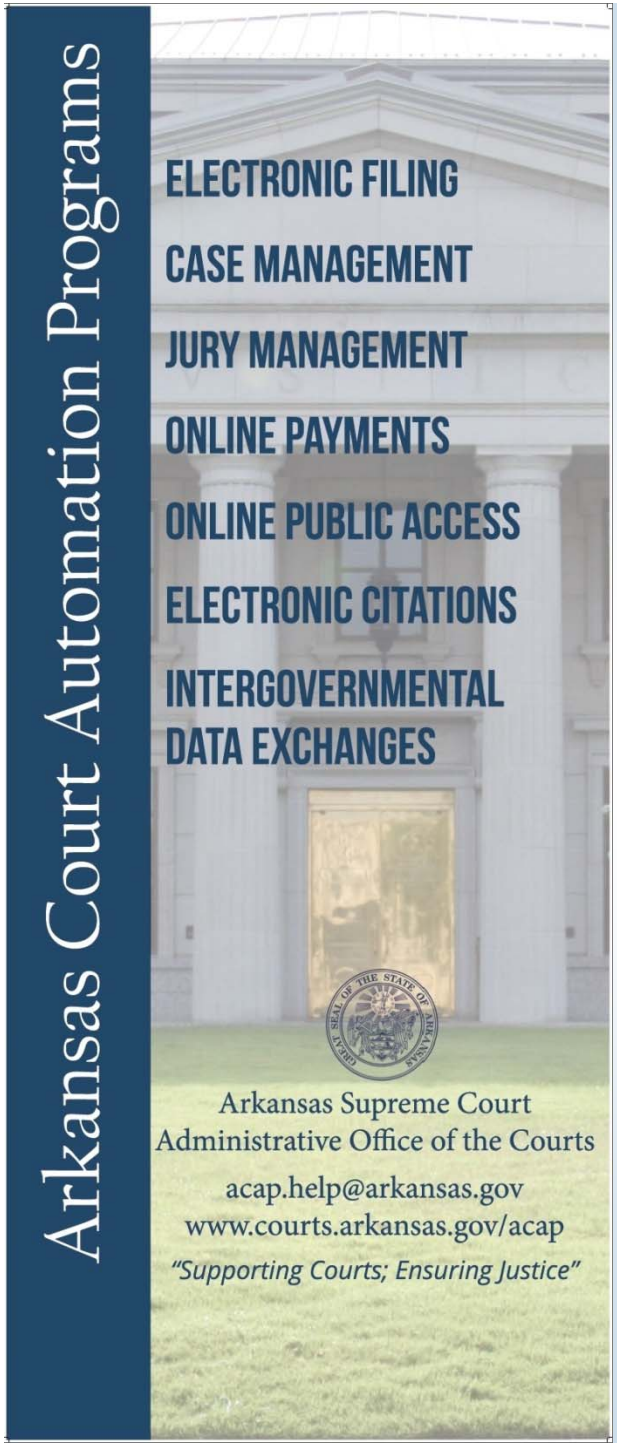



# 2016 ACAP Systems Conference

*"Supporting Courts; Ensuring Justice"*

# Do You Have Change For a Bitcoin?

Dain Couch
Arkansas Supreme Court
Administrative Office of the Courts
July 2016

# Agenda

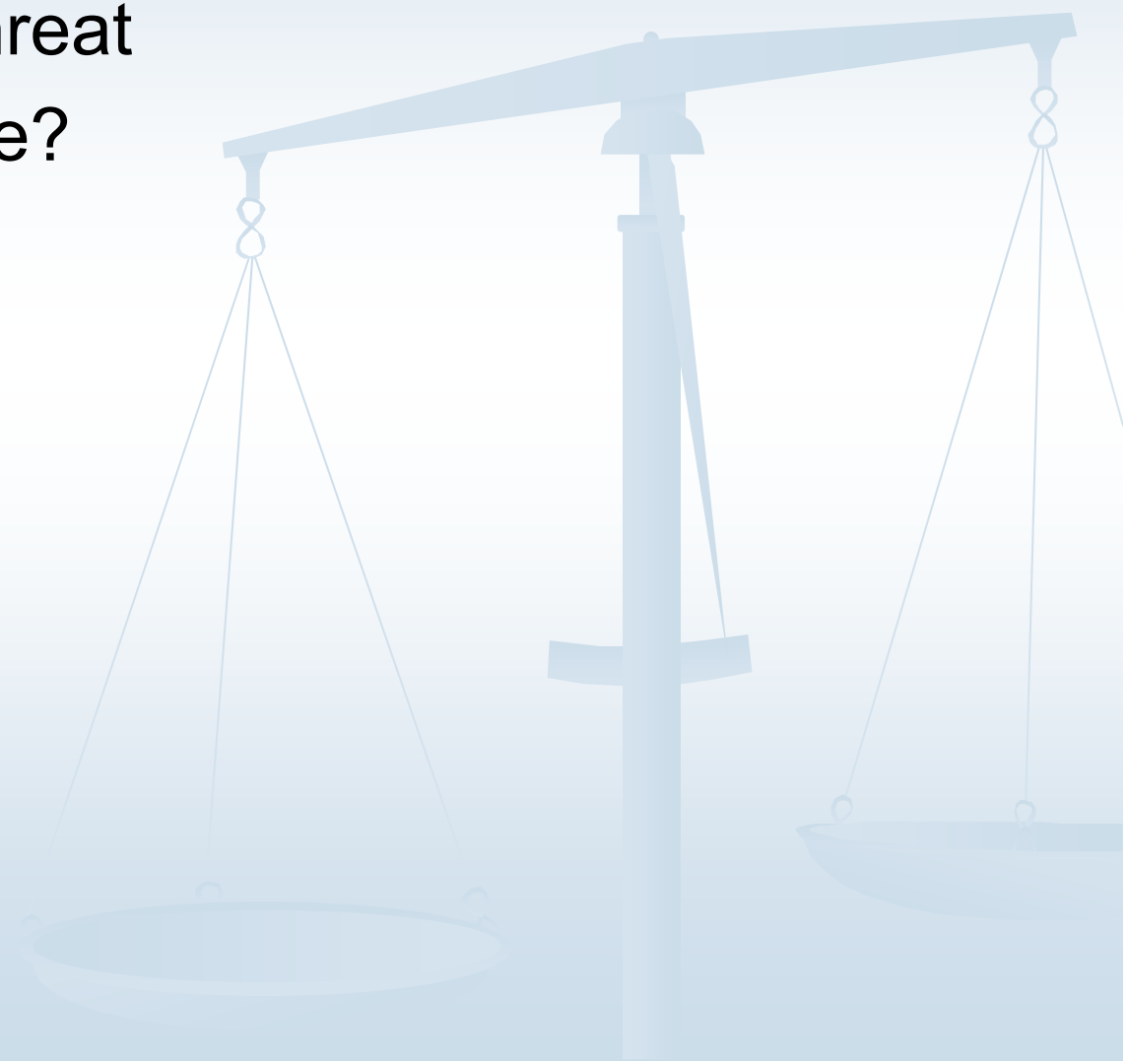
- What is a bitcoin?
- Cybersecurity Threats
- Steps you can take
- Legislative Audit
  - Application Checklist
  - Network Checklist

# Bitcoins

- What is a bitcoin?
- Why bitcoins?
- How do I get bitcoins?

# Ransomeware

- Latest, greatest threat
- Why ransomeware?
- Recent incidents
- Close to home



# Extortion

## Fake hackers extort $100,000 in bitcoin committing no attacks

26 April 2016 Hits: 903

Companies have paid more than $100,000 in bitcoin as ransom to a group of blackmailers in order to prevent cyberattacks. In fact, fraudsters have not made a single hack.

The group of alleged hackers, who call themselves Armada Collective, have been sending messages to various businesses, threatening to break into their systems unless they pay a ransom. Cybercriminals insisted on using bitcoins as a payment method. Their typical letter reads:

> "Your network will be DDoS-ed starting [date] if you don't pay protection fee — 10 Bitcoins @ [Bitcoin Address]. If you don't pay by [date], attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack."

http://www.coinfox.info/news/5387-fake-hackers-collect-more-than-100-000-in-ransom

## Ransomware is no joke, but sometimes, amateur attackers use 'pretend' ransomware -- and you can get your data back easily

By Fahmida Y. Rashid | Follow
InfoWorld | Apr 29, 2016

RELATED TOPICS
Security | Malware | Cyber Crime

1 COMMENT

INSIDER

**Public cloud megaguide: Amazon, Microsoft, Google, IBM, and Joyent compared**

The top five public clouds pile on the

Unlike most malware, ransomware is not stealthy. It's loud and obnoxious, and if you've been infected, the attackers will tell you so in no uncertain terms. After all, they want to be paid.

"Your personal files are encrypted," the message on the computer blares. "Your documents photos, databases, and other important files have been encrypted with strongest encryption and unique key, generated for this computer." While the language may vary, the gist is the same: If you don't pay the ransom -- typically within 48 to 72 hours -- your files are hosed.

**[ Oh no! Got real ransomware? Then one of these tools might help. | 4 reasons not to pay up in a ransomware attack. | Safeguard your data! The tools you need to encrypt your communications and Web data. ]**

Or are they? There is a slim possibility the perpetrators may be trying to fake you out and the files haven't been encrypted. While not a common scenario, it does happen, according to industry experts. Rather than paying up, you can bypass the scary fake message and move on with your day.

http://www.infoworld.com/article/3062552/security/how-to-tell-if-youve-been-hit-by-fake-ransomware.html

# Hactivism

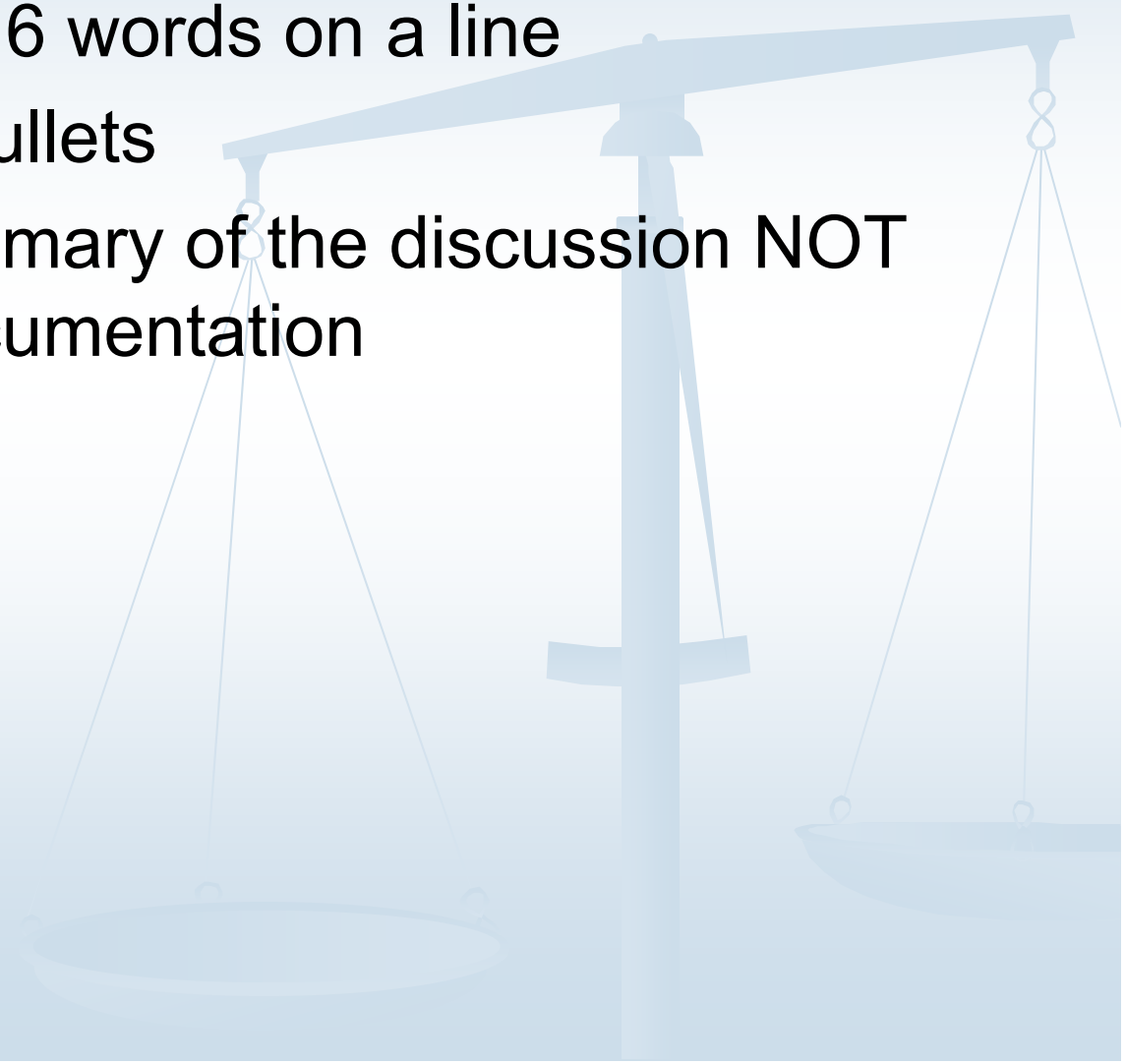
- What is hactivism?
- Why is it a threat to us?
  - Transgender
  - Abortion
  - Gun Control
  - Death Penalty
  - Racism

# Foreign Actors

- Target Government Organizations
- Cybersecurity Powerhouses
- ISIS - AR Librarians

# Targets of Opportunity

- No more than 5 – 6 words on a line
- No more than 3 bullets
- The PPT is a summary of the discussion NOT word for word documentation



# Insider Threat

- Unintentional
- Intentional

# Phishing

- What is phishing?
- Effectiveness

# Steps to Take

What can courts do?
What can you do?

# Prevention

- Firewalls
- IPS
- Antivirus
- Software Updates
- User Training

# Detection

- IDS
- SIEM

# Legislative Audit

- IT Best Practices
- Application Checklist
- Network Checklist

# Application Checklist

- Contexte is assessed
- User access
- Account reviews

# Network Checklist

- Court responsibility
- Accounts
- User access
- Virus protection
- Disaster Recovery
- Backups

# Questions?