Accounting & Financial Women's Alliance: AFWA

Friday, March 21, 2019

Arizona Country Club
5668 E Orange Blossom Ln
Phoenix, AZ 85018

Present:
Dealing with Digital Forensics Evidence
In
Financial Investigations

Presented by:

Scott Greene, SCFE, CEO

Evidence Solutions, Inc.

An Computer Forensics Firm

866-795-7166

Scott@EvidenceSolutions.com

Faculty:

Scott Greene
Evidence Solutions, Inc.
866-795-7166
Scott@EvidenceSolutions.com

"Digital Evidence, Data & Security"

Digital Evidence

ASWA

Scott Greene
Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

- Famous Quote
  - "I think there is a world market for maybe five computers." -- Thomas Watson, chairman of IBM, 1943
  - Today there are: over 1 billion PC type machines.

- "Digital Evidence, Data & Security"

esi evidence solutions, inc.

- The Commute
  - Enter your car without a key
  - Make periodic cell phone calls
  - Check in with On-Star
  - Two way GPS navigation effortlessly routes you around tie ups
  - You buy gas with your fast pass
  - You pickup your medications
    - and walk out without stopping at a cash register

- "Digital Evidence, Data & Security"

What potential trail have you left behind?

- Your car unlocked with a proximity sensor.
  - Near Field Communication
  - It is used to unlock vehicles when the Keyless remote fob is nearby
  - What if someone else was tracking that?
  - Near field communication is also a wireless phone technology that would allow you to make payments for products from your cell phone

- "Digital Evidence, Data & Security"

What potential trail have left behind?

- Cell phones with GPS
- Your carrier may have a database of where you have been
- Cell phone records are kept for.... well it depends

- "Digital Evidence, Data & Security"

What potential trail have left behind?

- Toll booths certainly tell a tale.
  - Smart Toll booths / near field communication
- OnStar
  - Currently only tracks your location when you call or are in an accident
  - They know your GPS coordinates

- "Digital Evidence, Data & Security"

What potential trail have left behind?

- Two way GPS navigation systems
  - Know your GPS coordinates
  - Even one way GPS systems can learn your habits and predict your route
- Buy gas with your fast pass
- Drug register-less purchase (RFID)

- "Digital Evidence, Data & Security"

Security!

- "Digital Evidence, Data & Security"

esi evidence solutions, inc.

- On the Internet….
  - Nobody knows you're a dog.
  - And increasingly, nobody knows you're a hacker.

A Juniper Research report indicates there will be 16,000 data breaches which will cost over $2 Trillian.

- "Digital Evidence, Data & Security"

- “Know the enemy, and know yourself, and in a hundred battles you will never be in peril”
  - -These prophetic words, spoken over 2,500 years ago by renowned - Chinese general Sun Tzu

- "Digital Evidence, Data & Security"

What potential trail have left behind? (Elsewhere)

- Copy Machines?
- Scanners?
- Fax Machines
- Old Computers!!!!!

- "Digital Evidence, Data & Security"

esi evidence solutions, inc.

- General
  - Cables
  - Access
    - Hotels
    - Airports (TSA)
  - Cars & Trucks
  - Etc.

- "Digital Evidence, Data & Security"

- Encryption!
  - Dance like no one is watching. Encrypt like everyone is!
  - Laptops
  - Cell Phones
  - Portable devices
  - Email? – Not normally, YET!

- "Digital Evidence, Data & Security"

- Hacking & Data Vulnerability
  - Keep Systems Patched!
  - Use a local firewall (Not Microsoft)
  - What about your mechanic?

- "Digital Evidence, Data & Security"

- Private Browsing!
  - Use it, but don't rely on it.

- "Digital Evidence, Data & Security"

- Artifacts From Web Browsing
  - The value of seeing what a person is searching for in the Internet can be key.

- "Digital Evidence, Data & Security"

- Artifacts From Web Browsing
  - http://wiki.answers.com/Q/How_can_you_help_a_sociopath?#slide=59
  - How can you help a sociopath? - Answers.com

- "Digital Evidence, Data & Security"

- Storage & Long Term Data Warehousing
  - Scanning and document destruction
    - Cloud accounts for long term storage
    - Local hard disk drives for storage
  - ESI & Personally
    - I keep no paper personally, except for deeds
    - And other similar types of documents
  - Use compatible formats
    - PDF
    - JPG
    - TIFF
  - Cloud Storage
    - Confidentiality?
    - Encrypt before you upload
    - Google Accounts
      - Is there some real risk of compromise of our data?

"Digital Evidence, Data & Security"

esi evidence solutions, inc.

- Malware
  - 70,000 new malware strains are detected every day.
  - Patches eliminate most of them

- "Digital Evidence, Data & Security"

- People People People
  - Organizations with educated users have fewer problems.
    - Threats to organizations
      - Social engineering
      - Sloppy users
      - End users are fooled into opening attachments and loading software from untrusted sites, visiting web sites where they are infected and more.
      - System administrators are also fooled like normal users but are also tested when:
        - unauthorized accounts are set up on their systems, when unauthorized equipment is attached, when large amounts of data are exfiltrated.

- "Digital Evidence, Data & Security"

- Mitigation
  - Train user to be wary of unsolicited attachments, even from people you know - Just because an email message looks like it came from a familiar source, malicious persons often "spoof" the return address, making it look like the message came from someone else.

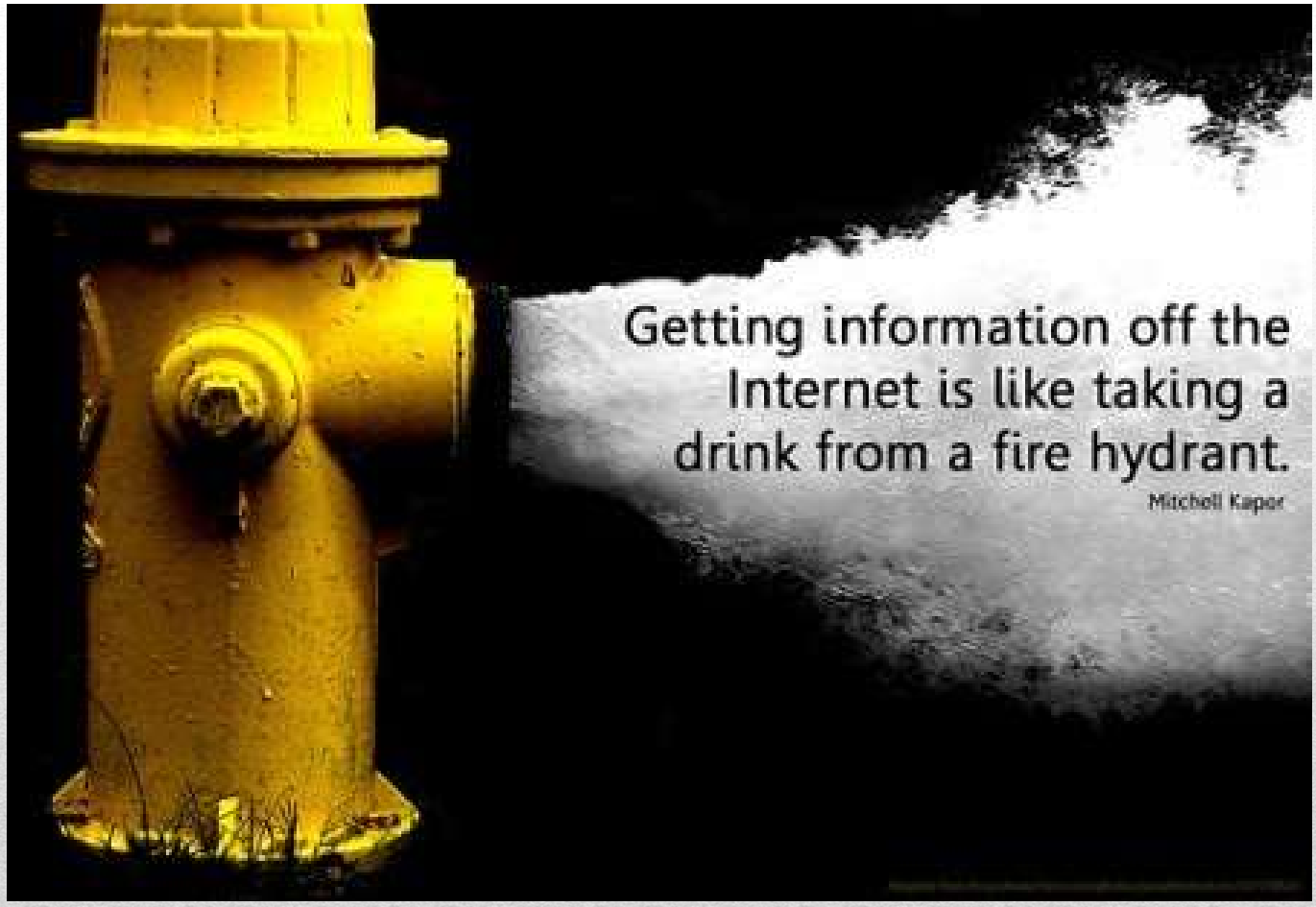
- "Digital Evidence, Data & Security"

- Mitigation
  - Check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This also includes email messages that appear to be from your Internet Service Provider (ISP) or software vendor claiming to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.

- "Digital Evidence, Data & Security"

- Mitigation
  - Teach your everyone to trust their instincts
    - - If email or attachment seem suspicious, don't open it, even if your antivirus software indicates that the message is virus free.
    - Attackers are constantly releasing “zero-days” and most likely your anti-virus software does not have a signature for it yet.

- "Digital Evidence, Data & Security"


Getting information off the Internet is like taking a drink from a fire hydrant.
Mitchell Kapor

- Metadata
  - Metadata is “data about data.” Metadata can be attached or associated with various types of ESI including: Document Files, Photos, SMS Messages, Messages, as well as physical items such as CDs and DVDs.

- "Digital Evidence, Data & Security"

- Metadata
  - Photographs
  - Electronic Medical Records
  - Vehicles
  - Email
  - Documents / Spreadsheets
  - File System Metadata

- "Digital Evidence, Data & Security"

- Evidence Collection Sources of Evidence:
  - Storage Media includes:
    - Hard Disk Drives
    - Floppy Disks
    - Backup tapes
    - CD Rom disks
    - E-prom and Memory chips
    - Thumb Drives
    - iPpods, iPads & MP3 Players
    - Cell Phones

- "Digital Evidence, Data & Security"

- Cell Phones & Tablets
  - Text messages
  - Photos?
    - GeoTagging
  - Calendars
  - Phone Books
  - Call Logs
  - Complete information about where the phone has been….

- "Digital Evidence, Data & Security"

- Cell Phones & Tablets
  - Browsing History
  - Documents
  - Email accounts
  - Online data storage accounts

- "Digital Evidence, Data & Security"

esi evidence solutions, inc.

iPhone Data After iOs 8

- **iCloud Backup**
- **Local Computer Backups**
- **Other**

- "Digital Security"

Android Data

- **On Phone Backups**
- **Local Computer Backups**
- **Cloud Backups**
  - **Searches, Sites, Etc**
- **Other**

- "Digital Security"

Do This:

- Personal Firewalls
  - Zone Alarm
  - Comodo
  - Norton Internet Security
  - Bit Defender
  - McAfee Internet Security

- "Digital Security"

Do This:

- Personal Firewalls
  - Zone Alarm
  - Comodo
  - Norton Internet Security
  - Bit Defender
  - McAfee Internet Security

- "Digital Security"

- Physical theft/loss
  - Phones and laptops are stolen:
    - More often from offices than from homes.
    - More often from cars than homes.
  - People:
    - Are lazy
    - They lose stuff
    - Steal Stuff

- "Digital Evidence, Data & Security"

Do This:

- Physical Theft / Loss - What's to be done:
  - Encrypt Devices
  - Backup data
  - Lock devices up

- "Digital Security"

There are a number of applications that can be installed on cell phones to prevent texting and driving.

- **DriveOFF – Free**
- **DriveMode – Free**
- **TextBuster - $179**
- **DriveScribe - Free**

- "Digital Evidence in Injury Cases"

esi evidence solutions, inc.

esi
evidence solutions, inc.

Scott Greene, President &
Senior Technology Examiner

866.795.7166 (toll free)
520.722.6796 (fax)

www.evidencesolutions.com
info@evidencesolutions.com

Scott@EvidenceSolutions.com