Minnesota Human Trafficking Task Force

Dakota County Electronic Crimes Task Force

April 25, 2022

What I did in my youth is hundreds of times easier today. Technology breeds crime.

(Frank Abagnale)

What is the DCECTF?

- The Dakota County Electric Crimes Unit (ECU) is a collaborative effort between most Dakota County Law Enforcement Agencies.
- We have 1 deputy, 3 police officers, and 2 civilians that are assigned to the unit.
- The Task Force handles digital evidence from all member agencies. Including cell phones, computers, vehicles, GPS devices, and security cameras.

Grant Funded

- In 2015 the Dakota County Sheriff's Office received a Grant through to hire a forensic examiner to work domestic related cases.
- In 2017 the Dakota County Sheriff's Office received a Federal Grant through the Office of Violence Against Women Act to help improve criminal justice responses to sexual assault, domestic violence, dating violence, and stalking. It also helped to fund a full-time position at the ECU to prioritize these types of cases.
- Since the Grant came to an end in late 2020, Dakota County Sheriff's Office created a full-time position within the ECU to continue to prioritize these types of cases.

General Procedure

- If a case that is submitted to the ECU is domestic related/stalking, the case would be worked first.
- We worked with agencies who submitted the victim's devices for examination to get the devices returned to the victim as quickly as possible to lessen the impact of not having a phone.
- We also try to provide assistance to advocates working with domestic violence related victims. This has included presentations with safety tips for digital devices and online activity.

Dakota County Electronic Crimes Task Force (DCECTF)

- Technology that we have found used for Stalking and Domestic Violence Related Crimes
  - Computers
  - Cell Phones
  - GPS Tracking Devices
  - Security Cameras
  - Shared Family Plans
  - E-mail Accounts and Social Media
  - Cloud Storage

DCECTF Cases

- We have identified keyloggers and spyware that were installed onto computers and cell phones.
- We have tracked suspects accessing victim's accounts, such as Google or iCloud; This allowed them access to location history, e-mails, calendar entries and documents.
- We have been able to find indications that a suspect had attached a GPS tracking device to a car.
- We found indications that a suspect attempted to hack into a server in the home for access to video cameras.

Technology Investigations

- Victim Devices:
  - Communications from the suspect
  - Signs of keyloggers, spyware or other snooping software installed on the device
- Suspect Devices:
  - Communication to victim
  - Information about the victim
  - Information related to accessing of victim's accounts
  - Attempts to hack into remote device
  - Receiving data from keyloggers
  - Purchase and researching of tools that can be used for stalking

Spyware/Keyloggers

- Allow others to see what is happening on the device
  - Messages and e-mails
  - Logins and passwords
  - Web browsing and purchasing
  - Phone calls
  - May be able to turn on microphone or camera to record
  - Pictures and Videos on phone
  - Location
  - Screenshots can allow anything that is on the screen to be seen
  - Record characters that are typed

Spoofing

- Spoofing is when a person masks their communication to make it appear as if it comes from someone else. This can be done with phone numbers and e-mails.
- Phone Spoofing:
  - This changes the caller ID, making it so that the text message or phone call appears to come from a different number
  - There are now services like Google Voice which allow a user to create a different phone number for free.
    - These are not technically spoofing
    - They allow a different phone number to be used on a cell phone
    - It does not have to be associated to person but there will be an e-mail associated with the account
- May be able to find evidence of these on suspect device

GPS Devices

- What can they do?
  - Real-time tracking using the Internet or a mobile app
  - Data is accessible from anywhere
  - Data may be stored for long periods of time (SpyTec stores data for a year)
  - Get notified when someone enters or leaves a pre-defined area
  - View data in Google Maps for ease of viewing
  - May track data about when the car is moving or stopped and what speed it is moving

Location Data

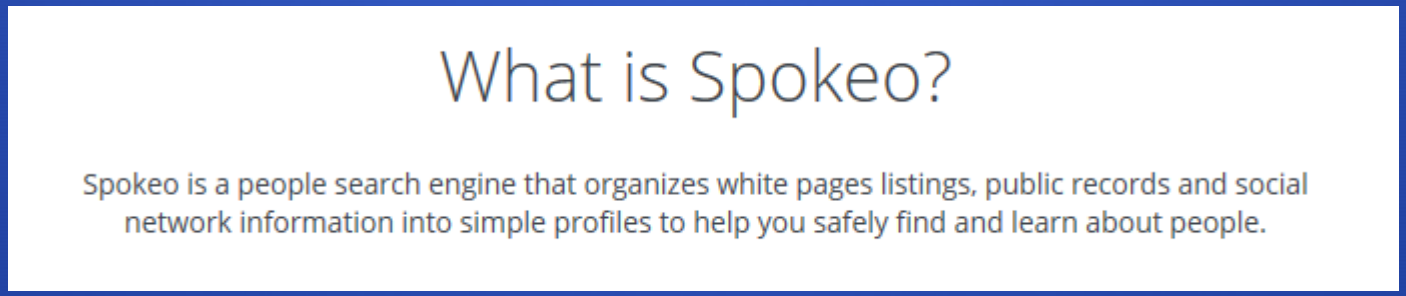
- Cell phones have GPS capabilities built-in
  - Spyware installed on a device can use these GPS capabilities to allow for tracking
  - Family plans for cell phone service may allow for tracking of devices
  - Family accounts such as Find My iPhone or Google Family may have family locator apps
  - Pictures taken with a cell phone may contain GPS data
  - Phone apps may use GPS data
- Location data may be shared on Social Media sites
  - Pictures or posts that indicate a location
  - May automatically report if "check-in" somewhere

Cameras

- Home Security System
  - Cameras and whole systems can be accessed remotely
  - Is the password known by others?
- High quality cameras are small and inexpensive
  - Requires physical access to install
  - Can be hidden in almost anything
  - Many can be accessed via apps or the Internet

Online Data

- There is a lot of information about people on the Internet.
  - Google a name to see what is out there
  - Data aggregators, such as spokeo.com, pull data from all over the Internet, including social media; Use one of these sites to see what information is available on a person
- Review the data available online and make sure there is nothing that is not wanted out there.



Social Media

- Social Media accounts are a great way to stay in touch with people, but they can also be a source of a lot of personal information
  - When a post is created it may display location information
  - Checking-in will detail a location at a given time
  - Pictures may also be used to identify a location
  - It's not just what is posted to a person's own account, but what people are tagged in by others

Accounts

- Family phone sharing plans
- Google or Apple Family accounts
- If a password is known or can be easily guessed then it is simple to login to someone else's account and see all of their data