Welcome to the Mac SIG Meeting
May 24, 2016

Ransomware /
Using iPad's Photos App

Ransomware

- **Standard antivirus approach doesn't work!** *(following is from Business Insider}*

  Antivirus software often works by maintaining a massive database of digital signatures of known viruses. The software scans your hard drive for these "fingerprints" and if it finds a file that matches known malware, it will attempt to quarantine and delete it. While this can protect your computer against well-known viruses, it won't do you much good if a virus is too new or obscure to be in a database. Plus, some viruses encrypt or modify their own source code, making it much harder for antivirus software to detect it.

  For detecting previously unknown viruses, we can now turn to heuristic analysis. Antivirus software that uses heuristic analysis can detect previously unknown viruses by studying the behavior of software running on a user's machine. If suspicious activity is detected, like the encrypting of the user's documents, the questionable software can be stopped in its tracks and removed.

Ransomware

- **How does ransomware work?** *(following is from Business Insider}*

  a) Initial ransomware infection: typically via an email attachment, a malicious download or installed by other malware;

  b) Getting comfy: ransomware alters the relevant registry keys and files to make sure its code is running when the computer runs;

  c) Calling home: malware calls the attacker's server to get encryption keys and register the attack;

  d) Doing the dirty work: it then proceeds to encrypt the user's files using the key obtained from the attacker's server;

  e) Making some noise: ransomware displays ransom notices and links that allow the victim to access websites accepting payment in Bitcoins.

Ransomware

- **What does ransomware look like?** *(following is from Business Insider}*

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

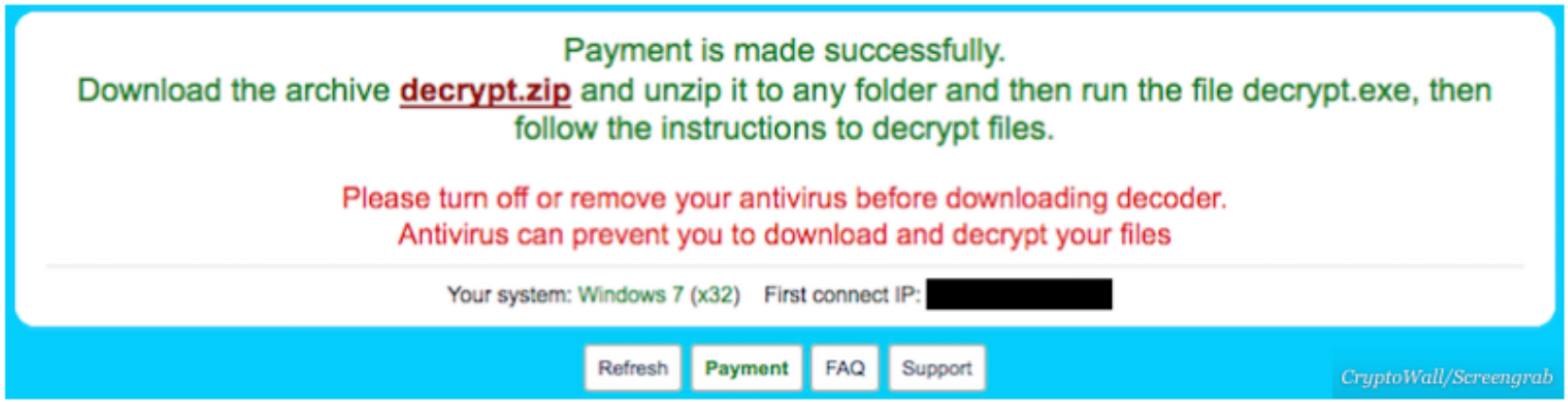
How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

In this screenshot provided by a CryptoWall victim, the virus explains what has happened to the user's files.

Ransomware

- **What does ransomware look like?** *(following is from Business Insider}*



A website associated with the CryptoWall ransomware virus provides decryption instructions to a victim who paid over $500 for the key.

Ransomware

- **How can one guard against it?** *(following is from Business Insider}*

a) The best approach to fighting ransomware say the experts is to avoid it in the first place by …..

Avoiding suspicious websites, emails, and files while online and using common sense and a healthy dose of skepticism;

b) Keep your operating system, antivirus, and installed software up to date at all times.

c) Keep backups of your files, preferably stored offline where they can't be reached by infections that make it to your computer.

d) Newer software and programs are starting to appear which claim that they limit ransomware. Some are a part of an antivirus program. However, the problem is that they can't combat it 100 percent and the hackers could eventually learn how to get around the software anyway.

Ransomware

❖ **How can one guard against it?** *(following is from Business Insider}*

a) The best approach to fighting ransomware say the experts is to avoid it in the first place by …..

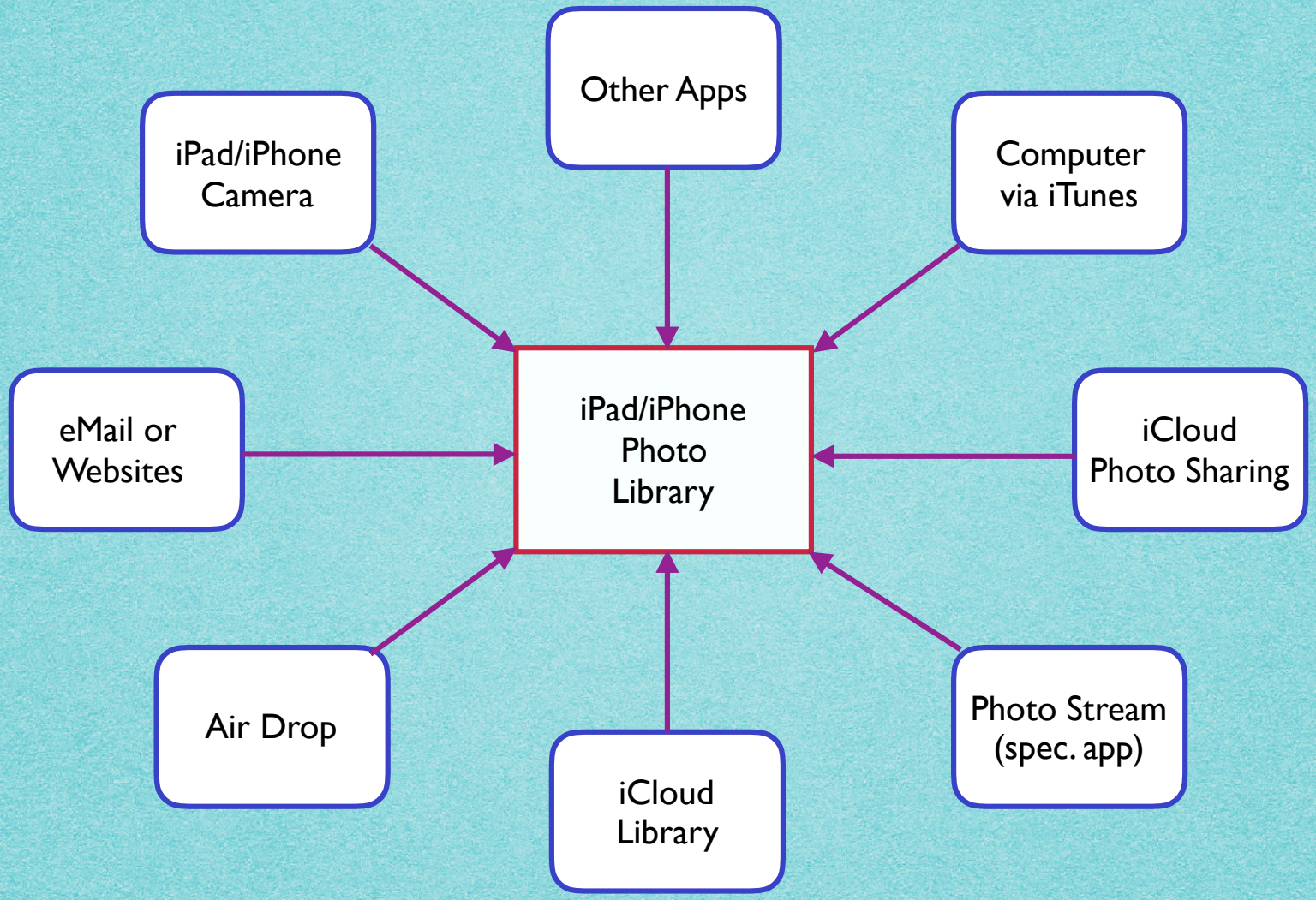
Avoiding suspicious websites, emails, and files while online and using common sense and a healthy dose of skepticism;

b) Keep your operating system, antivirus, and installed software up to date at all times.

★ c) Keep backups of your files stored offline where they can't be reached by infections that make it to your computer. This can be the cloud or a separate disc or drive unit.

This works best of all

d) Newer software and programs are starting to appear which say that they limit ransomware. Some are a part of an antivirus program. However, the problem is that they can't combat it 100 percent and the hackers could eventually learn how to get around the software anyway.


Other Apps
iPad/iPhone Camera
Computer via iTunes
eMail or Websites
iPad/iPhone Photo Library
iCloud Photo Sharing
Air Drop
iCloud Library
Photo Stream (spec. app)

Camera icon - You take pictures with this app

Photos icon - With this app you view pictures, edit them and/or transfer them to other places

When taking pictures on an iPad or iPhone, photos are automatically saved to the Photos app. They are saved chronologically then placed into 3 categories:

a. **Years**

b. **Collections**

c. **Moments**

Years is at the top level; Collections is next down; then Moments

Years

↓

Collections

↓

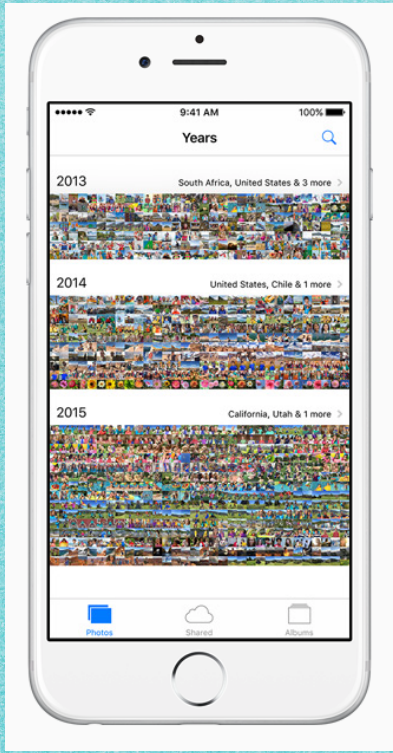
Moments

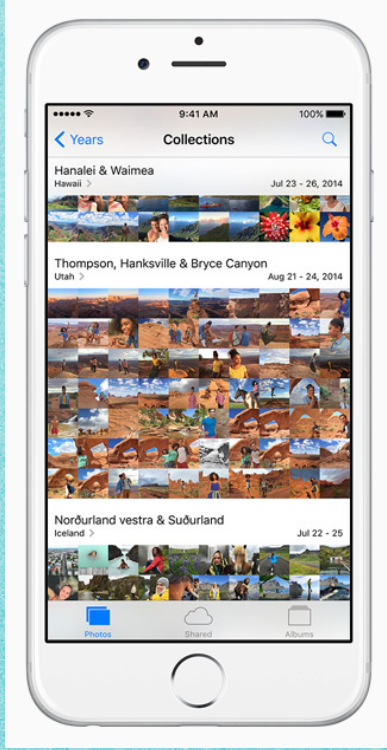
1. Assuming you take a lot of pictures, you would typically to start with the year that you took the picture(s) in: 2016, 2015, etc.

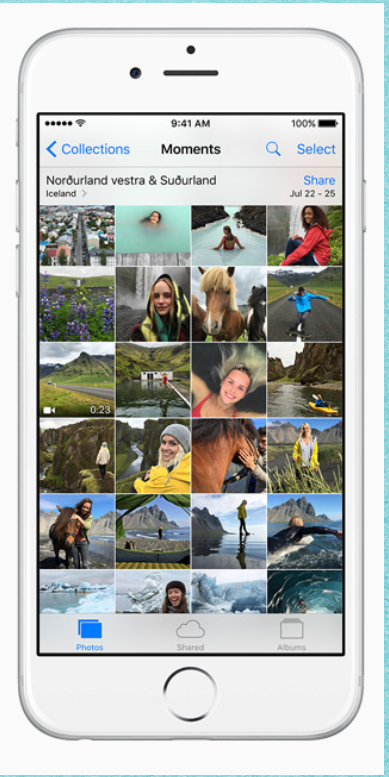
2. Then go to Collections where you can see a group of pictures taken at a certain place for a period of time. For example, a week at Lancaster, Wrightsville, Japan or Germany.

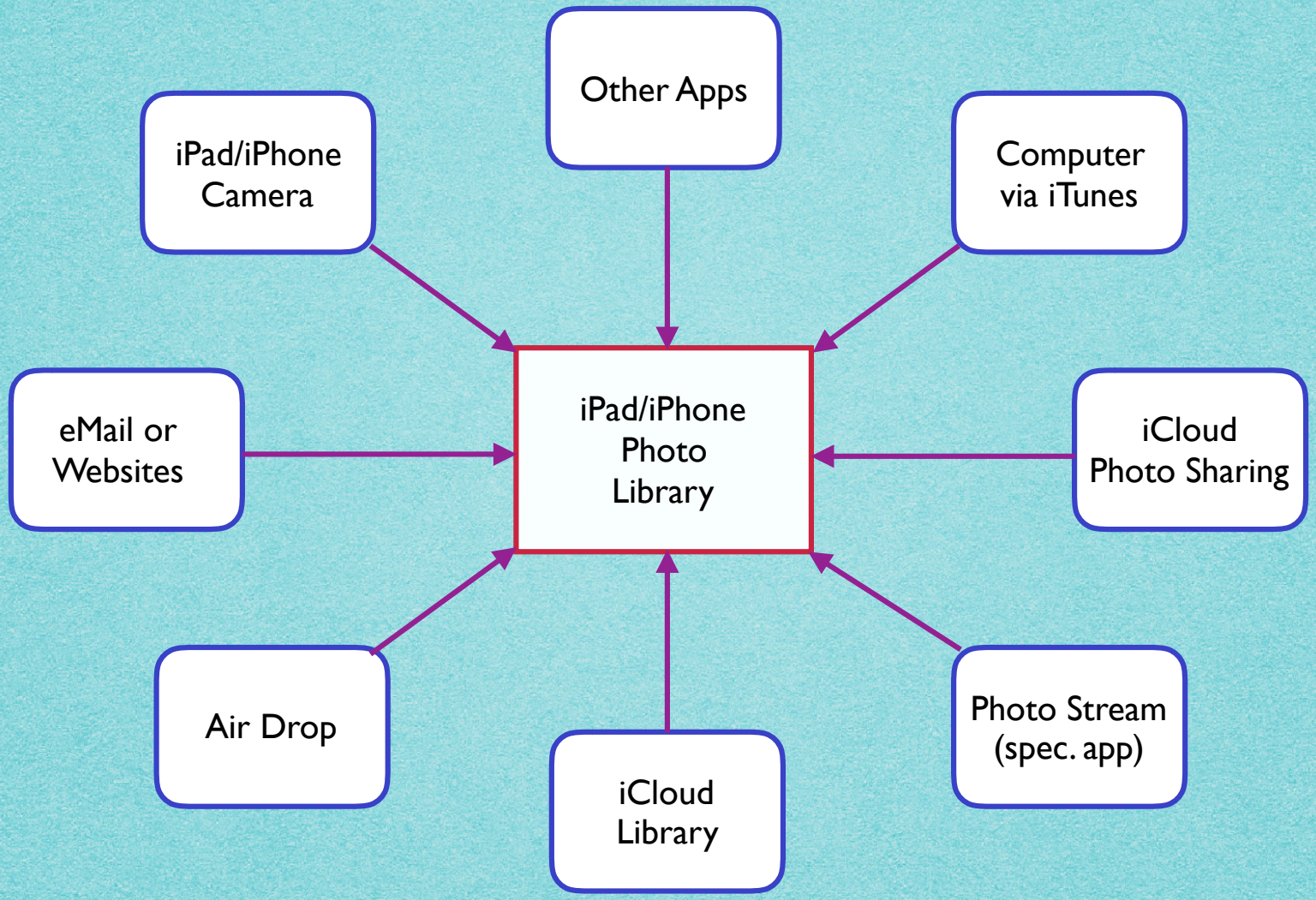
3. You then could go to Moments where a certain number of pictures were taken on a particular day or place. For example August 3, 2016 at the Belvedere restaurant in Lancaster.

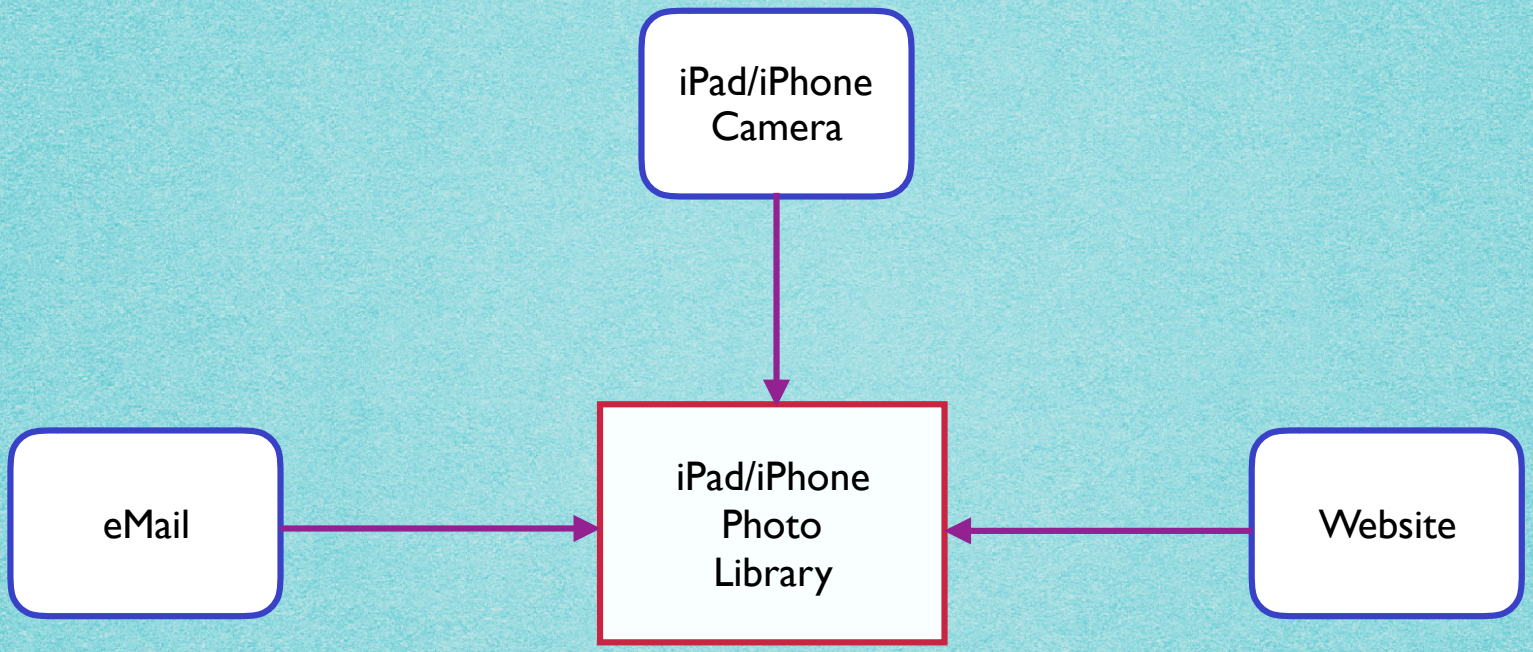
- Photos that are taken can show up in more than one place at the same time.
- How this occurs is a function of the Photo app and is based on dates and locations.
- Having categories helps to keep things organized if you take lots of pictures.
  A person can more easily get to the photo that they want to see.








Other Apps
iPad/iPhone Camera
Computer via iTunes
eMail or Websites
iPad/iPhone Photo Library
iCloud Photo Sharing
Air Drop
iCloud Library
Photo Stream (spec. app)


iPad/iPhone
Camera
eMail
iPad/iPhone
Photo
Library
Website