

# How Secure is My Device

**APCUG Security  
Virtual Technology Conference  
October 17, 2015**

**Jere Minich, APCUG Advisor, Region 5  
jminich (at) apcug.org**



# What Devices will I cover?

- PC's – Windows 7, 8/8.1, 10
- Tablets – Android, iPads
- Smart Phones – iPhone, Android

# I am not at risk ?

- There is malware out there targeting every mobile platform:
  - Apple iOS
  - WinMobile
  - Blackberry
- The vast majority of mobile malware programs today target Google Android users

# The Infection Cycle

1. The Hacker generates a program and puts it on the Internet or in email.
2. Your anti-virus company discovers the hacker's program.
3. The anti-virus company writes a software program to block or delete the hacker's program.
4. You get an update from the anti-virus company, usually daily.
5. You install the update – some are auto-installed.

**What is the Time span from Step 1 to 5.?**

**Bottom Line – everyone can get infections.**

# Symptoms of Malware - PC

- Sudden - Poor Performance
- Lots of Stuff running in the Background
- The Following Programs fail to work:
  - Task Manager
  - Anti-virus Program
  - Regedit = Registry Editor
  - System Restore
  - Msconfig = System Configuration

# Symptoms of Malware – PC

## Unwanted Changes

- Can't turn off a toolbar
- Can't delete a Toolbar
- Browser Home Page Changes
- Search Engine Page Changes
- **Assume that your Antivirus has been compromised**
  - Scan with something else
    - Eset Online Scanner – [www.eset.com/online-scanner](http://www.eset.com/online-scanner)
    - Trend Micro Housecall – [www.housecall.trendmicro.com](http://www.housecall.trendmicro.com)
    - **Neither program requires installation**

# Symptoms of Malware Mobile Devices

- Noticeable performance issues
  - Everything taking longer than usual
- Using up data at a faster rate than before
- Battery seems to be running down much faster
- Calls being dropped or interrupted with weird noises
- Unwanted behaviors
- Frozen apps
- Failure to reboot
- Difficulty connecting to the network
- Racked-Up Phone Bills

# Cell Phone Terms

- IMEID = International Mobile Equipment Identity
- ICCID = Integrated Circuit Card Identity
- MEID = Mobile Equipment Identity
- 3G = Third Generation cell phone signals – speed
- 4G = Fourth Generation - + High Speed Packet Access
- LTE = Long Term Evolution – a standard for wireless communication of high-speed data for mobile phones and data terminals
- SIM Card = **s**ubscriber **i**dentify **m**odule – 3 sizes
  - Standard; Micro; Nano
- Major Cell Phone Networks =
  - CDMA – Verizon & Sprint - Code division multiple access = USA
  - GSM – AT&T & T-Mobile- Global System for Mobile Communications  
= Most of the world
- Note: 5C, 5S & 6 iPhones contain antenna for both = World phone =  
Going overseas = call carrier



# The 15-digit serial or IMEI number helps to identify your phone and can be accessed by:

(International Mobile Equipment Identity)

- keying **\*#06#** into most phones
- looking behind the battery of your phone
- checking in the phone's settings
- **Make a note of this number and keep it separate from your phone:**
  - as this number could help to trace and prove ownership quickly if it is stolen
- If you report your phone stolen, the service provider should then be able to stop further use of your phone
- However, registering it means your phone usage is tied to your identity

# Security - Smartphone malware is easily distributed through:

- an insecure app store
- hidden in pirated versions of legitimate apps, which are then distributed through 3rd party app stores
- an "update attack"
  - where a legitimate application is later changed to include a malware component
  - which users then install when they are notified that the app has been updated

# Information is vulnerable when sent from a mobile phone

- Each mobile phone provider has full access to:
  - all text and voice messages sent via its network
- Phone providers are legally obliged to keep records of all communications
- Voice and text communication can also be tapped by third parties in proximity to the mobile phone, using inexpensive equipment

# Information is vulnerable within the sender's and the recipient's phones

- Mobile phones can store all sorts of data:
  - call history
  - text messages sent and received
  - address book information
  - photos
  - video clips
  - text files
- Modern mobile phones are pocket-sized computers
- With more features comes higher risk
- **In addition, phones that connect to the Internet are also subject to the insecurities of computers and of the Internet. (Malware)**

# Phones give out information about their location

- As part of normal operation, every mobile phone automatically and regularly:
- informs the phone service provider where it is at that moment
- Many phones nowadays have GPS functions,
- and this precise location information may be embedded in other data such as:
- **photos,**
- **instant messages**
- **and internet requests that are sent from the phone**

# What are the different kinds of infections?

- **Malware** – a general term - malicious software disguised as legitimate software
  - designed to collect and transmit private information
    - such as passwords, without the user's consent or knowledge
- **Viruses** – program replicates by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive
  - Can create a **BotNet**
  - **Botnet = Robot Network**
- **Worms** - a stand-alone malware program that actively transmits itself over a network to infect other computers.

# What are the different kinds of infections?

- **Rootkits** – stays concealed, to avoid detection; invisible in the system's list of processes
- **Backdoors** - bypass normal authentication procedures; usually over a connection to a network such as the Internet
- **Trojan Horses** - a program disguised as something normal
- **Ransomware** – restricts access to the system that it infects, and demands a ransom paid

# How does Malware get into my device?

- Security defects in software –
- Malware exploits security defects
  - security bugs or vulnerabilities
- in the design of the:
  - operating system
  - applications (Apps)
  - browsers
    - browser plugins such as:
      - Adobe Flash Player
      - Adobe Acrobat
      - Adobe Reader
      - or Java



# Basic Security Setup for Android Devices

## Access to your phone

**Step 1.** Set up **Sim Card Lock**, found under: System > Security > Sim and Lock Settings.

you must enter a PIN number in order to unlock your SIM card each time your phone is switched on

**Step 2.** Set up a **Screen Lock**, found under: System > Security > Screen Lock

which will ensure that a code, pattern or password needs to be entered to unlock the screen

**Step 3.** Set the **security lock timer**: which will automatically lock your phone after a specified time of no action

specify a value which suits you, depending on how regularly you are willing to have to unlock your phone

# Basic Security Setup for Android Devices

## Device Encryption

**Step 4.** If your device uses latest Android version you should turn on **device encryption**

- This can be done in: Settings > Security > Encryption
- Before you can utilize device encryption, you will be required to set a screen lock password

**Note:** Before starting the encryption process, ensure the phone is:

- fully charged
- and plugged into a power source

# Basic Security Setup for Android Devices

## Network settings

**Step 5.** Turn **off** Wi-Fi and Bluetooth

Ensure that Tethering & Portable Hotspots are switched off when not in use.

**Step 6.** If your device supports Near Field Communication (NFC), this **will be switched on by default**, and so must be **switched off manually**

# Basic Security Setup for Android Devices

## Location settings

**Step 7. Switch off** Wireless and GPS location:

under Location Services  
and mobile data

under data manager > data delivery

Note: Turn **ON** location settings as you need them. It reduces:

the risk of location tracking,

saves battery power

reduces unwanted data streams initiated by applications running in the background or remotely by your mobile carrier

# Basic Security Setup for Android Devices

## Step 8. Caller Identity

If you want to hide your caller-ID, Go to:

Phone Dialer > settings > Additional Settings > Caller ID  
> hide number

# Often-overlooked Security Settings for iPhone and iPad

- Check privacy controls = Settings > General > Privacy
- Enable Find My iPhone = Settings > iCloud > Find my iPhone/iPad
- Separate your iTunes and iCloud passwords = do not use the same
- Enable a Passcode = Settings > Passcode > Require Passcode
- Enable Erase Data – ten attempts = Settings > Passcode > Erase Data

# Often-overlooked Security Settings for iPhone and iPad

- Turn on Find My iPhone/iPad - incorporated a new technology called "Activation Lock," which is effectively Apple's version of the Kill Switch
- Enable Backup Encryption – found in iTunes
- Keep iOS Updated – iOS 9.0.2 = Settings > General > Software Update = update with Power Plugged in.
- Disable Bluetooth = Settings > Bluetooth > Turn it Off

# Often-overlooked Security Settings for iPhone and iPad

- Enable Fraud Warnings & Pop Up Blocker = Settings > Safari
- Restrict purchases and media content = Google all purchases for safety/security
- Use Find My iPhone Activation Lock = Settings > iCloud > Google it.
- Control what's displayed on the lock screen = Settings > Notifications Select
  - manage certain categories
- Block unwanted calls and texts on iPhone = Recent > select > Scroll Down to Block
- Enable Do Not Track (DNT) in Safari and block cookies



# Often-overlooked Security Settings for iPhone and iPad

- View a link's URL before tapping it – press and hold
- Enable - Lost Mode
- Maintain Physical Security – keep it close to you.
- Do Not Jailbreak your iPhone or iPad
  - lowers security,
  - disables the enforcement of code signatures,
    - which is an important security feature

# Often-overlooked Security Settings for iPhone and iPad

- **Do Not**

- Join **Untrusted** Wireless Networks.
- Allow less secure apps to access your account.
  - Some examples of apps that do not support the latest security standards include:
    - applications that send your credentials directly to Gmail
    - digital credential = proof of qualification, competence, or clearance that is attached to a person
    - credentials may contain personal information such as the person's name, birthplace, birthdate, and/or biometric information such as a picture or a finger print

# What to do about downloading Apps

Check app reviews.

- always read the reviews first.
  - If the app is problematic in any way, some of the reviews will make note of it and you can move on.
  - If the app doesn't have any reviews, you may want to steer clear until it does.

Check developer's track record.

- check the developer's other apps to see if they have a reputable track record.

Be wary of third-party app markets.

- all app markets have some degree of risk to them.
- stick to the reputable App stores.

Be careful when granting Superuser privileges.

- limit Superuser privileges only to the apps you trust 100%.
- If you grant Superuser access to every app that asks for it, then you're just asking for malware to gain full control of your device.

Run malware scans regularly.

- schedule scans.
- make a routine out of scanning, whether it's once a day or once a week.

# Email & Malware

- Email 'attachments' containing malware are the most common way attackers get into your device, such as:
  - a file sent along with an email message
    - You can see all attachments in email – 'file extension'
  - Pictures
  - .exe files ( a common filename extension denoting an executable file)
  - Some viruses use files with two extensions to make dangerous files look like safe files.
  - For example, Document.txt.exe or Photos.jpg.exe

# Email Protective Measures

- **Delete** - suspicious emails with attachments
- **Disable** –Wi-Fi & Bluetooth when you are not using them
  - **Beware** of “disguised” attachments
  - Example: Hogcaller.gif.exe
- **Keep** email software up-to-date
  - Use alternative email software - ‘client email’ vs ‘Web Email’
    - Microsoft Outlook , Mozilla Thunderbird , Eudora. (‘Client’ Email Programs)
- **Disable** automatic reading of emails
  - ‘Webmail’ - make sure that your email provider offers an antivirus tool

# How to avoid trouble in Email

- If in any doubt, **don't open it**
- **Delete** anything from someone you don't know
- **Never:**
  - click on anything from an unknown source
  - open an attachment from an unknown source
  - download from an unknown source

# Keeping All Software up-to-date

- Keep your apps up-to-date at the pace you want
  - When security vulnerabilities are discovered by the OEM:
    - they are patched with security updates
- When you have auto-update turned on:
  - apps that require new permissions in the latest update will always require your confirmation before updating
  - regardless of the setting
- All Software - should be kept up-to-date
  - with the newest security updates
- It keeps you safe

# How to keep Software/Apps Updated

- Check for Updates to your device
  - Go to Settings
  - Click on Software Updates
- Connect your device to its Power Source
  - Do not update Operating System while running on battery
- Connect to the Internet and the Program Website
  - Click on Updates
- Google Search- software update checker for android; iPad; iPhone; etc.



# Here's how to update your apps on Android

- Find the Android Marketplace on your home screen;
  - or in your app drawer
- Tap it to open it up
- Once the Android Marketplace loads:
  - tap the menu button on your device
  - choose the 'My Apps' option
- In a few seconds you should see a list of your apps
- If there are available updates you'll see red/orange text that says Update to the right of the app's name
- Tap Update All at the top of the screen to update your apps
- You can update them individually by tapping and holding down the app you want to update and then choosing Update from the resulting menu

# Best Update Checker tools – PC's

- Ninite Update Checker
  - [www.ninite.com](http://www.ninite.com)
- Secunia PSI (Windows, Free)
  - [http://secunia.com/vulnerability\\_scanning/psi-android/](http://secunia.com/vulnerability_scanning/psi-android/)
  - [http://secunia.com/vulnerability\\_scanning/personal/](http://secunia.com/vulnerability_scanning/personal/)

# Simple Prevention

- Never click to “accept terms” from any company without reading the fine print
  - Accept may = access address book and forward a message to everyone in it!
  - EULAlyzer Personal
    - <http://www.brightfort.com/eulalyzer.html>
- Use **antivirus** software and keep it up to date
  - 1 program only
  - No reasonable difference between free and \$\$
  - Run Weekly Quick Scans
  - Run Monthly Full Scans

# Simple Prevention

- Be cautious of the internet
- Avoid:
  - misleading ads
  - strangers with offers
  - strange e-mails
  - questionable websites
- Do Google search to verify

# Tools to remove Malware – PC

in addition to your anti-virus

- Use a Malware Removal software program
- **Malwarebytes** – best on the internet- for mobile Android
  - <https://www.Ninite.com>
- **Malicious Software Removal Tool** – Microsoft tool
  - <http://www.microsoft.com/security/pc-security/malware-removal.aspx>
- **Spybot Search & Destroy** (Windows, Freeware)
  - <http://www.safer-networking.org/private/>

# Secure versus unsecure site

- Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network used on the internet:
  - prevents wiretapping and man-in-the-middle attacks
  - provides bidirectional encryption of communications between a client (you) and server
- iPads & iPhones = a padlock in the URL bar.

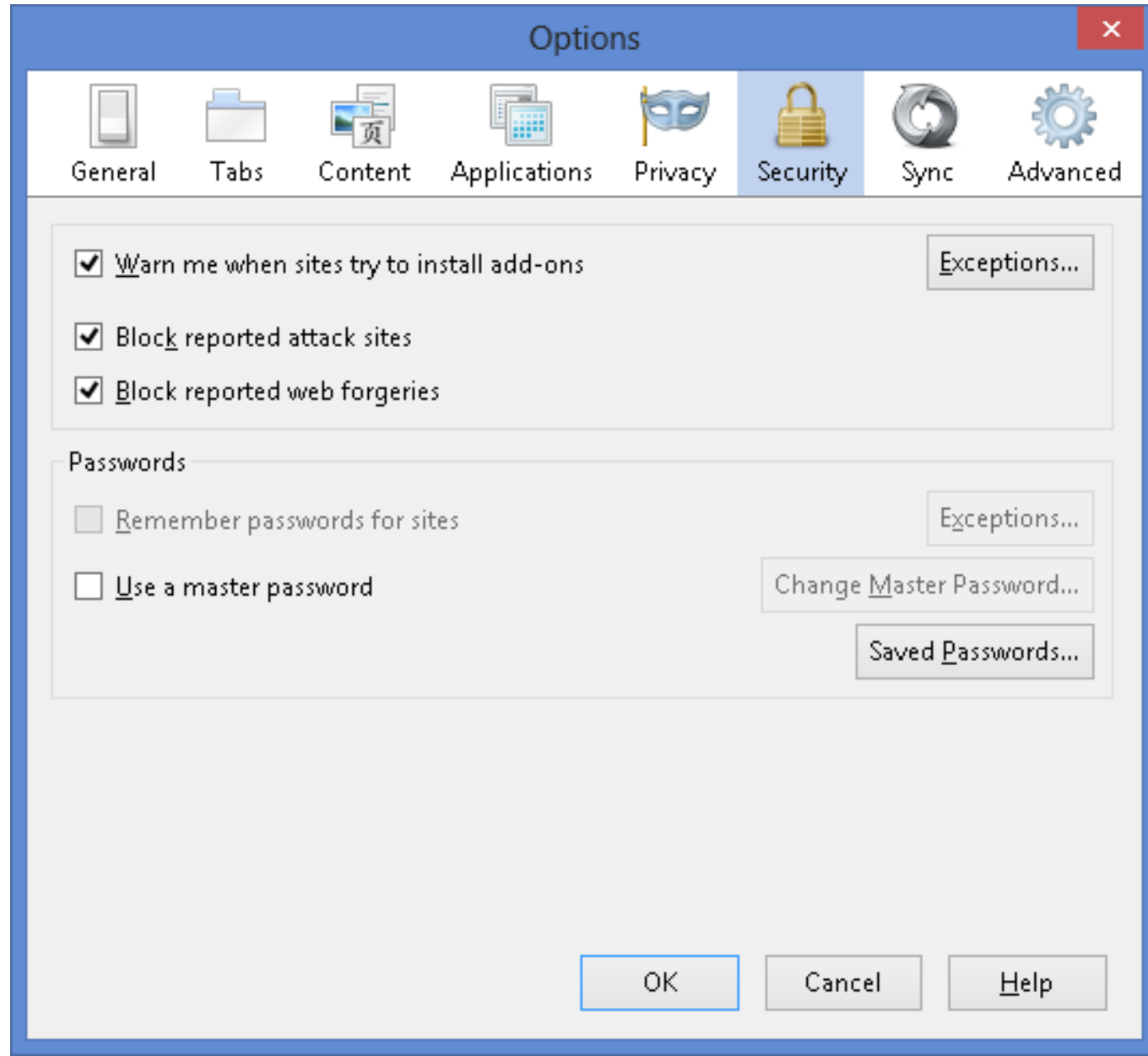
# Programs to have on your Computer

## My personal selection

- One (1) Antivirus – free is OK
  - Microsoft Security Essentials ( Windows 8 = Windows Defender)
  - **Run Scan Weekly**
- A Firewall – Software on Computer / Hardware in Modem Router
- A Malware Removal Program
  - Malwarebytes - Free or Annual Charge of \$25.00
  - **Run Weekly**
- A Scanning Program
  - Spybot Search and destroy
  - **Run Weekly**
- An Advertisement Blocker
  - Ad-Aware
  - **Run Weekly**

# Setting Security in your Browser

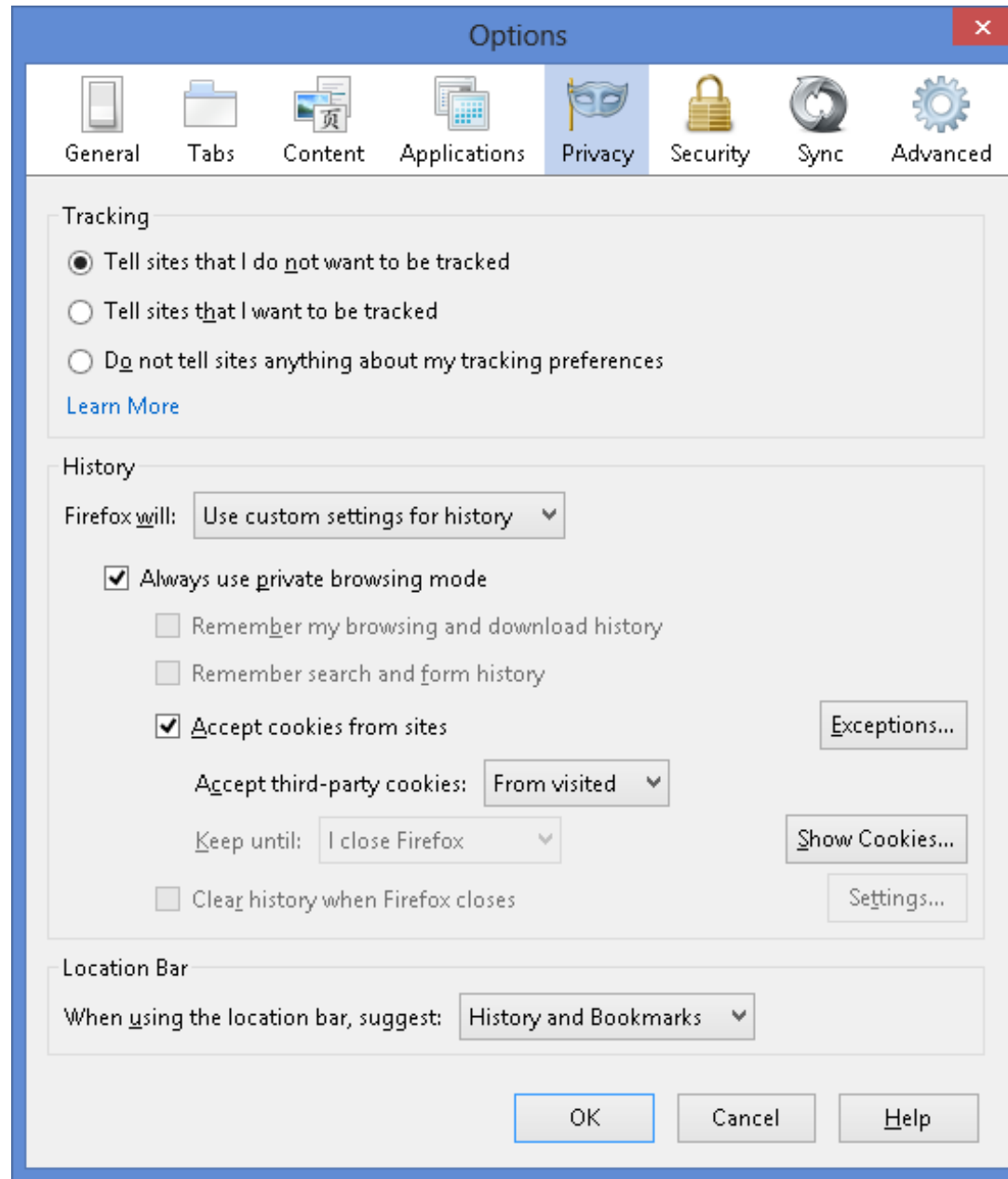
On the  
Menu Bar:  
Tools:  
Options:  
Security Tab





# Setting Privacy in your Browser

Tools:  
Options:  
Privacy Tab



# Bottom Line

- **You** must control your Security – run your own security software.
  - ISP Anti-virus for free = you're not sure it is running or up-to-date.
- Keep Software up to date- OS, Anti-virus, Scanners, Ad-Aware.
- Run Quick Scans weekly and Full Scans monthly.
- Do **NOT** 'Open' or 'Go To' a web page or email if you are not sure.
- Do **NOT** pass-on Emails – “pass this to everyone” emails you may get.
- Do **NOT** allow access to your Contact list – some apps want that.
- Stay Alert when on the Internet.

# Questions?

Jere Minich  
APCUG Advisor, Region 5  
Jminich (at) apcug.org

