Who I Am

• Supporting Macs, iPads, iPhones and all things Apple since 1988

• In business as Gentle Computer Helpers since 1999

• 🍇 Certified Support Pro
Target Audience

• People using iPads for personal use (at home, around town or traveling)
• People in business for themselves
• People working in a small organization
Those With Different Needs

- Those working in journalism, academia, government, law, military, banking, investment, medicine, etc.
- Activists or whistle-blowers
- Those at risk of bullying, stalking, assault, abuse or legal action
- Those of interest to nation-states or large organizations
What is Security?

• The means (hardware, software or human) to delay or reduce the risk of

• the loss of data, access to services or ability to use our iDevice

• due to internal defects or external dangers.
What We Can Do

• Set things up in a secure fashion.
• Customize settings.
• Change the way we ordinarily do things.
• Be alert for specific threats when they are most likely.
Apple’s iOS Security Guide

• Authoritative reference for iOS hardware and software: how it all works.

• For IT departments, provides the behind-the-scenes technical details.

• Available at:

Physical Security

• Get a protective case.
• Keep it away from, higher than, liquids.
• Keep possession. Think twice before giving it up.
• Shut it down if you can’t.
• Always put it in the same place. Put it back when done.
Get A Protective Case

• Dramatically reduces the risk of physical damage.

• Highly protective cases aren’t more unattractive, bulky or expensive.

• For comprehensive, unbiased reviews and comparisons, see:

  http://www.mobilereviews-eh.ca/
iOS Passcode

• Essential protection whenever iDevice not in your possession

  1) Settings > Touch ID & Passcode > Change

  2) > Passcode Options (longer or alphanumeric)

• Write it down, store in password manager

• Give it to executor
Poor Passcodes

• Many pick a poor passcode:

http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes

Don’t use:
• Repeated or sequence of numbers (0000, 123456)
• Dates (1948, 011998)
• Numbers that correspond to words (5368 = LOVE)
• A geometric pattern (1397, 147852)
Strong Passcodes

Strong passcode are:
• Longer (at least 6 numbers)
• Random
• Alphanumeric (but harder to enter)

Numerical passcodes longer than 6 characters still use the number keypad

Can roll dice to create a strong passcode:
• 1st: odd up from 1; even down from 0
• 2nd die: the number (6 doesn’t count)
• e.g. 3,2=2; 4,2=9; 1,6=roll over
TouchID - Pros & Cons

• Must still remember passcode!
• More convenient, faster
• Harder to steal (peeking or surveillance cameras don’t work)
• Easier to compel entry (physically and legally)
Other Touch ID Uses

- Approve purchases from iTunes, App Store, iBooks (instead of your Apple ID password)
- Apple Pay
- Authenticate apps, e.g. 1Password
TouchID - Set Up

- Settings > General > Touch ID & Passcode
- Use 3rd or 4th finger of the hand you don’t usually use to tap icons
- To increase reliability, create several fingerprints of that single finger in slightly different positions
Still Must Enter Passcode

• Just been turned on or restarted.
• Not been unlocked for more than 48 hrs.
• Received a remote lock command.
• After 5 unsuccessful Touch ID attempts.
• Set up new fingerprints with Touch ID.
Lockdown the Lock Screen

Settings > Touch ID & Passcode

- Disable all access when locked
- Enable Erase Data to automatically wipe it after 10 failed passcode attempts

Settings > General > Auto-Lock > 1 Minute
Update iOS

Why?

• Fixes bugs (things that don’t work due to programming errors)

• Addresses security vulnerabilities

Let’s look at some security vulnerabilities
iOS 9.3 fixed...
The Security Content of iOS 9.3

Apple maintains a list of recent security updates with links to their content here:


The security content of iOS 9.3 is here:

https://support.apple.com/en-us/HT206166

• Each entry lists the CVE ID = the Common Vulnerabilities and Exposures ID
Reveal User’s Location

- WebKit

Impact: Visiting a maliciously crafted website may reveal a user's current location

Description: An issue existed in the parsing of geolocation requests. This was addressed through improved validation of the security origin for geolocation requests.

CVE-2016-1779 : xisigr of Tencent's Xuanwu Lab (http://www.tencent.com)
Terminate App or Execute Code

• FontParser

Impact: Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution

Description: A memory corruption issue was addressed through improved memory handling.

CVE-2016-1740 : HappilyCoded (ant4g0nist and r3dsm0k3) working with Trend Micro's Zero Day Initiative (ZDI)
Execute Code as Kernel

- **Kernel**

  Impact: An application may be able to execute arbitrary code with kernel privileges.

  Description: Multiple memory corruption issues were addressed through improved memory handling.

  CVE-2016-1754: Lufeng Li of Qihoo 360 Vulcan Team
  CVE-2016-1755: Ian Beer of Google Project Zero
# Vulnerabilities Addressed by iOS 9.3

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute arbitrary code</td>
<td>17</td>
</tr>
<tr>
<td>Execute arbitrary code with kernel privileges</td>
<td>6</td>
</tr>
<tr>
<td>Terminate application unexpectedly</td>
<td>11</td>
</tr>
<tr>
<td>Track sensitive user information</td>
<td>3</td>
</tr>
<tr>
<td>Denial of service</td>
<td>3</td>
</tr>
<tr>
<td>Malicious website can display an arbitrary URL and read cached contents</td>
<td>1</td>
</tr>
<tr>
<td>Others</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>49</strong></td>
</tr>
</tbody>
</table>
Why Update Quickly?

• Once Apple issues an update, the vulnerabilities are public.

• Malicious individuals or organizations can determine what Apple fixed.

• They can attack devices which are not yet updated.
Update iOS Expeditiously

• Back up your iDevice first.

• Install incremental updates (e.g. 9.x) immediately. At least within 2 days.

• For major releases (e.g. iOS 8 -> iOS 9), I still recommend you upgrade immediately.

• If you want to be cautious, wait for the first incremental update (e.g. 9.1).
Busy? Install Tonight or Remind Later

Secure Your iPhone & iPad

Gentle Computer Helpers

4/9/2016
What Do Security Experts Do?

Figure 4: More experts than non-experts reported installing software updates in a timely manner.

Make Update Alerts Visible

- Place Settings, App Store icons on Home Screen.
- Red circles with numbers on icons indicate available updates.
Back Up

- Protects against hardware damage, failure, or loss
- Protects against software corruption.
- Can return software and data to previous state.
- Can transfer apps and data to another device.
iDevice Backup Options

• To iCloud via Wi-Fi:
  - When on, locked, connected to power
  - Settings > iCloud > Backup > Backup Now

• To computer through iTunes
  - Apple cannot access
  - Enable Encrypt backup to copy all data
  - Make it the same as your Apple ID password to make it easy to remember)

For more info and directions go to:
https://support.apple.com/en-us/HT203977
## iOS Malware 2009 - 2014

<table>
<thead>
<tr>
<th>Name</th>
<th>Discovery date</th>
<th>Presumed origin</th>
<th>Devices</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS/Trapsms.APr.spy</td>
<td>June 2009</td>
<td>Russia?</td>
<td>Jailbroken</td>
<td>SMS Forwarder</td>
</tr>
<tr>
<td>Spy/MobileSpy/iPhoneOS</td>
<td>Aug 2009</td>
<td>USA</td>
<td>Jailbroken</td>
<td>Spyware</td>
</tr>
<tr>
<td>iOS/Eeki.Alworm</td>
<td>Nov 2009</td>
<td>Australia (Ashley Towns)</td>
<td>Jailbroken</td>
<td>Worm Proof of Concept</td>
</tr>
<tr>
<td>iOS/Eeki.Blworm</td>
<td>Nov 2009</td>
<td>The Netherlands</td>
<td>Jailbroken</td>
<td>Mobile banking malware</td>
</tr>
<tr>
<td>iOS/Toires.Alpr.spy</td>
<td>Nov 2009</td>
<td>Switzerland (Nicolas Seriot)</td>
<td>Any (jailbroken or not)</td>
<td>Rogue application - Proof Of Concept</td>
</tr>
<tr>
<td>Adware/LBTMTiOS</td>
<td>Sep 2010</td>
<td>France</td>
<td>Any (jailbroken or not) - Was found (and removed) in the official AppStore number</td>
<td>Call premium phone</td>
</tr>
<tr>
<td>Spy/iKeyGuard/iPhoneOS</td>
<td>Apr 2011</td>
<td>Czech Rep.</td>
<td>Jailbroken</td>
<td>Keylogger</td>
</tr>
<tr>
<td>iOS/FindCall.Alpr.spy</td>
<td>July 2012</td>
<td>Russia?</td>
<td>Any (jailbroken or not) - Was found (and removed) in the official AppStore</td>
<td>Privacy trojan</td>
</tr>
<tr>
<td>Riskware/KillmobiOS</td>
<td>July 2013</td>
<td>USA</td>
<td>Jailbroken</td>
<td>Spyware</td>
</tr>
<tr>
<td>iOS/AdThief.Altr</td>
<td>Mar 2014</td>
<td>China</td>
<td>Jailbroken</td>
<td>Ad revenue hijacking</td>
</tr>
<tr>
<td>iOS/SSLCreds.Altr.pws</td>
<td>Apr 2014</td>
<td>China</td>
<td>Jailbroken</td>
<td>Password stealer</td>
</tr>
</tbody>
</table>

Don't Jailbreak

Removes iOS software restrictions:

• Allows access to iOS file system and manager.
• Can install apps, extension, themes unavailable from App Store.

iOS restrictions ensure security:

• 8 of 11 malware apps depend on it.
• Hacking much easier without them.
Read App Reviews Before You Buy

Search the Internet:
• “app name” or “type of app” iOS review
• Look for reviews in MacWorld, Mac|Life, CNet, Lifehacker, PC Magazine, etc.

iTunes reviews
• Read bad and good
Check App Privacy, Settings

Once new app installed, check settings:

- Settings > Privacy > Location Services
- Settings > Privacy > Each built-in app
- Settings > [new app name]
Maintain Apps

Keep apps up-to-date
• Fixes bugs, plugs security vulnerabilities
• Place App Store icon on home screen

Delete unused apps
• Each installed app makes you more vulnerable

1. Tap and hold until jiggle
2. Tap small circle with X
An iPad User
<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Phone</th>
<th>Email</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jean H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miriam H</td>
<td>Seattle, WA</td>
<td></td>
<td>@gmail.com</td>
<td></td>
</tr>
<tr>
<td>Francis H</td>
<td></td>
<td></td>
<td>@gmail.com</td>
<td></td>
</tr>
<tr>
<td>The Hartford</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Her Credentials

• User Names similar to: m1ddleage
• Passwords similar to: s1LlibR0uneed
• Security Questions similar to:
  First Car? a blue unaSSembledVW sedan
What’s Good

- Unique passwords for each site.
- Passwords not words with numbers and/or special characters before or after.
- Password of moderate length (~12 chars)
- Security question answer long (26 chars)
What Could Be Better

Passwords
• Longer
• Random characters
• More special characters
• Easier to enter

Security question answers
• Unrelated to the question
• Or even better -> random characters

Could be lost or stolen
• Easily read by others
• No back up
Password Manager

• Can generate truly random passwords, user names, answers, etc.

• Can save passwords of any length.

• Built-in web browser.

• Can enter passwords, etc. automatically.

• Automatically backs up and syncs with other devices.

• Can’t be read or used without master password.
Why Not iCloud Keychain?

Interface hard to understand and use:
• May have multiple entries for same item.
• Includes many items user unconcerned with and confused by, e.g. certificates.

Once you open iDevice, it’s active:
• Doesn’t have its own password.
• Can require passcode for individual items.
1Password

- Beautiful, clear, easy-to-use interface.
- Data encrypted on devices and in iCloud.
- Apps for iPhone, iPad, Mac, Windows.
- Can unlock with Touch ID!

-> Buy from App Store so syncs via iCloud.
Apple ID Account - Security Services

An Apple ID provides access to Apple’s online services, some relevant to security:

1. Automatic backup over the Internet to Apple’s servers (iCloud) to protect data
   - due to hardware failure or software corruption
   - damaged, lost or stolen device
   - in case of potential ransomware attack
Apple ID Account - Security Services (2)

2. Can automatically sync your data sync to other Apple devices and iCloud account

• Contacts, Calendars, Photos, Notes, Reminders, iCloud Drive/Documents

• Helps ensure data is up-to-date, accurate, and accessible from many devices.

• BUT if someone gains access to your iCloud account, they control your data!
3. Find My iPhone protects you if your iDevice is misplaced, lost or stolen:

• Locate it on a map.
• Play a sound from your iDevice.
• Display a message on the lock screen.
• Remotely lock it and erase your data.

You’ll need your Apple ID and password to unlock and restore your apps, data.
iCloud Account Compromised

4/9/2016

Secure Your iPhone & iPad
Apple ID Account Vulnerabilities

“certain celebrity accounts were compromised by a very targeted attack on user names, passwords and security questions”

- Apple Media Advisory, Sept. 2, 1014

Apple ID Account

How your account is identified and verified:
• Apple ID
• Password
• Birthday
• Security questions
• Rescue email

We need strategies to protect them.
Protect Your Apple ID

- Must be a valid email address you control.
- Use your regular email, many will know it.
- Solution: set it up differently.

  1) Create an email account that you use only for your Apple ID. Nothing else!
  2) Turn on email forwarding from that account to your main email account.
Protect Your Apple ID (2)

• A good set up because others won’t know your Apple ID.

• Pay attention when you get Apple email.

Scammers send forged Apple email to trick you to go to a fake website and enter your Apple ID and password.
Protect Your Apple ID (3)

When "Apple" emails you, check "To:" field

From: Apple <noreply@insidecloud.icloud.com>
Subject: Your Apple ID was used to sign in to iCloud via a web browser.
Date: April 5, 2016 at 10:48:50 AM EDT
To: alcapone@gentlehelpers.com

Dear Michael Inskeep,

Your Apple ID (alcapone@gentlehelpers.com) was used to sign in to iCloud via a web browser.

Date and Time: April 5, 2016, 7:47 AM PDT

If the information above looks familiar, you can disregard this email.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) and change your password as soon as possible.

Apple Support

Forwarded to mike@gentlehelpers from alcapone@gentlehelpers.com
Protect Your Apple ID (4)

When clicking on a link in email, tap and hold lightly until the Open pop-up menu appears.

Confirm that the address in the pop-up matches and is valid.
Apple ID Password

Apple’s Minimum Requirements:

• At least 8 characters.

• At least 1 upper and 1 lowercase.

• At least 1 number.

But nearly everyone still picks a weak password!
Strong, Memorable Passwords

• Longer is stronger.
• Random is stronger.
• Embedded words make it memorable.
Pick Your AppleID Password

Use Diceware to create a strong password:

1) [http://world.std.com/~reinhold/diceware.html](http://world.std.com/~reinhold/diceware.html)
2) Roll 25 dice to pick 5 words (see diceware site).
3) Roll 2 dice to pick letter to capitalize (1st = word, 2nd = letter). Roll 3 more to add #.
4) Roll 4 dice to add a random character (see site).
5) Write it down or in 1Password, give it to executor.
Online Diceware Generator

• Or go to this site to generate a diceware password without using dice:
  https://entima.net/diceware/

• Thanks to Adam Rice for this suggestion!
Apple ID Security Questions

- Hackers guessed answers to Sarah Palin’s security questions, reset her password.
- Must be as hard to guess as password.
- Use 1Password or Diceware to pick long, random passwords as answers.
Rescue Email

- Second email address linked to Apple ID.
- Used to reset your security questions if you forget or lose the answers.
- Use your regular email address.
2-Step Authentication

• Links a trusted device (iPhone, iPad, Mac) to your Apple ID.

• When you sign in for the first time from a new device, you must enter password and 6-digit code sent to the trusted device.

• Even if someone gets your password, they can’t take over your Apple ID.

• Replaces security questions.
2-Step Authentication in Action

Apple ID
To finish signing in, enter the verification code sent to your other devices.

Didn't get a verification code?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 ABC</td>
<td>3 DEF</td>
</tr>
<tr>
<td>4</td>
<td>GHI</td>
<td>5 JKL</td>
</tr>
<tr>
<td>7</td>
<td>PQRS</td>
<td>8 TUV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Gentle Computer Helpers

4/9/2016
Secure Your iPhone & iPad
More on 2-Step Authentication

Get more info and instructions from Apple:
System Requirements

- iPhone, iPad, or iPod touch with iOS 9
- Mac with OS X El Capitan and iTunes 12.3
- Apple Watch with watchOS 2
- Windows PC with iCloud for Windows v5 and iTunes 12.3.3
Older Versions of iOS

• Can enable “2-step verification” for their Apple ID.

See: https://support.apple.com/en-us/HT204152
Enable 2FA for Other Accounts

Set up 2-step authentication* for all your accounts that support it.

Learn who else supports 2-step authentication:
https://twofactorauth.org/

*Also called “2-factor authentication” or “2FA”.
Enable iCloud Services

• Settings > iCloud

Enable at least:
• Contacts
• Calendars
• Backup
• Find My iPhone
Wipe iPhone Before Return, Repair, Resale

1. Back up. (The only way to recover data...)

2. Settings > General > Reset > Erase all content and settings

• Erases cryptographic keys, making all user data on the device inaccessible.
Wireless Networks

• Turn off Wi-Fi when you leave trusted location. (Can set reminder by location.)

• If you access public Wi-Fi, use a VPN.

• Disable Personal Hotspot in public: Settings > Personal Hotspot
Public Wi-Fi Is Not Secure

https://wifipineapple.com
Impersonates Wi-Fi Networks

Are you my preferred wireless network?

Yes

How The Wifi Pineapple Snoops

Virtual Private Network:
• Encrypts your communications.
• Verifies the identity of your host.
• Cloaks your location.
Virtual Private Network #1

Private Internet Access

- PC Magazine Editor’s Choice
- Many gateways in many countries so great performance
- works with Macs, iOS devices
- Reasonably priced by time period:
  - $6.95/month
  - $39.95/year

https://www.privateinternetaccess.com/
Virtual Private Network #2

Private Tunnel

• decent performance
• works with Macs, iOS devices
• iOS app
• priced by usage
  free/2 GB
  $10/20 GB
  $20/100 GB
  $30/unlimited/year

https://www.privatetunnel.com/
Bluetooth

• When it’s on, it’s another way to attack your iDevice

• Turn it off when you’re not using it:

  Settings > Bluetooth > Off
Safari for Browsing Set Up

Safari for ordinary browsing with settings:

**General**
- *Passwords, Autofill off; Block Pop-ups on*

**Privacy & Security**
- *Do not track, Fraudulent website warn on*
- *Allow cookies from current website*

Then before each browsing session:

**Advanced**
- *Javascript off* (unless needed for site)
- *Remove All Website Data* (before session)
Use 1Blocker

• Blocks malware, malicious content delivered via ads.

• Privacy from tracking scripts.

• Will reduce data downloaded so pages load faster, battery lasts longer.

http://1blocker.com
Use 1Password for Secure Browsing

- Any site where you need to sign in.
- Has its own built-in browser.
- Stores site addresses, user names, passwords, etc.
Monitor URL Bar

- Make sure the address shown matches your intended destination.
- Padlock indicates a secure connection. Only sign in, make purchases when displayed:

  🛠 www.google.com
Email Settings

In settings, enable SSL if provider supports:

- Your connection to the server is validated.
- Your username, password sent encrypted.
Links in Email

Confirm link address matches text by tapping and holding lightly on the link:

![Image of link address]

Date and Time: April 5, 2016, 7:47 AM PDT

https://appleid.apple.com/

- Open
- Add to Reading List
- Copy
- Cancel
Be Skeptical of Email Attachments

• Not requested? Not expecting it?

  -> Forward the message to the sender asking if they sent it. Do not use reply.

• Be especially leery of files ending in .zip, .doc, .docx, .xls, .xlsx, .ppt, .pptx
Apple Pay

iOS makes you MORE secure!

1. Enter credit card in Wallet app.
2. Check for Wireless Pay or Apple Pay.
3. Hold iPhone near terminal.
4. Place finger for Touch ID.
Apple Pay Terminal

Secure Your iPhone & iPad

4/9/2016

Gentle Computer Helpers
iPhone Pay Screen

Try Again

Pay with Passcode

Gentle Computer Helpers

4/9/2016
Secure Your iPhone & iPad
Experts vs Non-Experts on Security

What are the top 3 things you do to stay safe online?

- Update system
- Use unique passwords
- Use two-factor auth
- Use strong passwords
- Use password manager
- Check if HTTPS
- Don't share info
- Use antivirus
- Use Linux
- Use verified software
- Be suspicious of everything
- Visit only known websites
- Change password
- Delete cookies

Experts (N=231)  Non-experts (N=294)
Experts vs Non-Experts on Security

How good is this advice?

- Turn on automatic updates
- Install OS updates
- Be suspicious of links
- Don’t enter passwords on links in email
- Don’t open email attachments from unknown
- Update applications
- Use unique passwords
- Use strong passwords
- Use a password manager
- Use two-factor authentication
- Look at the URL bar
- Be skeptical of everything
- Don’t click links from unknown people
- Use antivirus software
- Check if HTTPS
- Don’t write down passwords
- Clear browser cookies
- Write down passwords
- Visit only known websites
- Save passwords in a file

Percentage of Experts (N=231)

- 5 (Very good)
- 4
- 3
- 2
- 1 (Not good at all)
- I don’t know

4/9/2016
Secure Your iPhone & iPad

Gentle Computer Helpers
No Phone While Driving

• Can’t control the vehicle while fiddling with your device.

• Hands-free “cell-phone drivers exhibited greater impairment than intoxicated drivers.”

http://psych.utah.edu/lab/appliedcognition/
No Phone While Driving Plan

• Set up driving directions before you start.
• Let calls go to voicemail or passenger.
• Pull over before accessing your phone.