The P U L P

Newsletter of the Hartford User Group Exchange

December 15th General Meeting:

Geek Toys

Knights of Columbus
2533 Main Street,
Glastonbury, CT

Q&A Session: 7 PM–7:15PM
Meeting starts at: 7:15PM

Member of

apcug

An International
Association of Technology
& Computer User Groups

Contents	Page
From the Editor	2
Stu's Quiz Page	3
Cybercrime and Phishing	4
The Illustrated iTunes License Agreement	5
How to See Your iPhone's Precise Signal Strength	6
What To Do If Your iPad/iPhone Is Taken	8
Calendar	10

MEETING LOCATIONS

East Hartford Public Library
Main & Central Avenue
in the Lion's Community Room
Downstairs

From The Editor

by Stuart Rabinowitz

This month's meeting is 'Gift suggestions for/to Geeks' (& others).

In the news: The switch to Macs from PCs has reportedly saved IBM $270 per user

There is a prototype "gizmo" that knows your Amex number before you've received your new card |

Cops pulled over a Google driverless car -- but not for speeding. It got pulled over for impeding traffic while going to slow. No ticket was issued.

Dell PCs root certificate security error widens as researchers dig deeper. It could open your PC to attack.

Yahoo Mail begins blocking users with ad block enabled.

Don't trust that USB drive!.

Fool's gold could mean faster-charging batteries.Also, longer-lasting, 3D solid-state batteries could displace lithium-ion.

Self-encrypting drives are hardly any better than software-based encryption.

Facebook will soon scan your smartphone to find photos of your friends.

Carbon nanotubes in a race against time to replace silicon.

First Linux ransomware program has been cracked, for now.

Apple might enable your iPhone with a secret way to activate 'panic mode'.

Beware bad USB-C cables, Google engineer warns —while naming names.

Winner claimed in $1 million iOS 9 hacking contest.

MIT researchers have used Wi-Fi to look through walls.

Send your comments to editor@huge.org

Happy computing!! Until next month...

Stuart Rabinowitz, Editor

Here is the appropriate copyright citation and a link to the full text. articles from "Tidbits"

http://creativecommons.org/licenses/by-nc-nd/3.0/

A Little Computer Quiz

Since October was "CyberSecurity Month", here are a few questions about those that created a need for it.

1 At age 13 he was [hacking ARPANET](#) and NASA for blueprints to decorate his wall and he used Scorpion as his login. Now there is a TV show based on his life. What is his real name?

2 In 2000 MafiaBoy launched a [series of DDoS attacks](#) against high-profile dot-com era sites like Yahoo! and E-Trade. What is is real name?

3 The cryptocurrency BITCOIN was created by Satoshi Nakamoto, any guesses?

4 Geohot wrote the first iOS jailbreak tool and reverse-engineered the PlayStation 3. What is his real name?

5 Rocky Clark was a hardware hacker that developed a black box for making free long distance calls. What is his real name?

Extra Credit: Believe it or not, there is an "Official Computer Freaks Joke Book" authored by Larry Wilde and ...?

Nov. Quiz Answers

1 This month marks the 34th anniversary of the founding of what nationally known computer user group?
  A the Hartford User Group Exchange -- HUGE.

2 Where was the first meeting held?
  A Computer City near Sears in West Hartford.

3 What were the original dues?
  A $10 a year

4 Who was the first President?
  A Richard Johnston

5 Who was the guest speaker at the tenth anniversary meeting?
  A Guy Kawasaki

Cybercrime and Phishing
By Kathy Frey, Member, Computer Club of Green Valley, AZ
Summer 2015 edition Green Bytes
www.ccgvaz.org
frey58 (at) cox.net

At one time or another we all will be a victim of some form of Cybercrime and Phishing. The use of any preventive product is of little help if you don't practice safe computing. Help protect yourself:

1. Watch out for "**phishy**" emails. The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. **Delete** them. Do not open them.

2. Don't click on **links** within emails that ask for your personal information.

3. Beware of "**pharming**." This was also known as **redirect**. In this version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you're taken to a fake site without realizing it. Malicious programs can be either spyware, adware or malware. Run your spyware scanning programs. Malwarebytes is a recommended program.

4. **Never** enter your personal information in a pop-up screen.

5. **Only open** email attachments if you're expecting them and know what they contain.

6. Phishing also happens by **phone**. You may get a call from someone pretending to be from a company or government agency, making various kinds of false claims and asking for your personal information. Quite often it is about some problem with your computer. There is no way they can possibly know if you even own a computer. If you have caller ID, screen your calls, and do not answer calls from phone numbers you do not recognize.

7. If someone contacts you and says you've been a victim of fraud, **verify** the person's identity before you provide any personal information. Get a phone number and call them back. Or call who they are supposed to represent and ask if that business is making those kinds of calls.

8. **Report phishing**, whether you're a victim or not. Tell the company or agency that the phisher was impersonating.

9. Don't be embarrassed, **take action** immediately if you've been hooked by a phisher. If you provided account numbers, PINS, or passwords to a phisher, notify the companies with whom you have the accounts right away. For information about how to put a "fraud alert" on your files at the credit reporting bureaus, contact the Federal Trade Commission's ID Theft Clearinghouse, www.consumer.gov/idtheft.

Most Recent Scam Alerts from the Federal Trade Commission:
Stand up to fake debt collectors - April 10, 2015
Unlocking the code - April 3, 2015
The FTC didn't send that sweepstakes letter - April 2, 2015
Scammers play name game and get caught - March 27, 2015
An invoice today gets the doctor to pay - March 26, 2015
Reluctant to be rude? - March 25, 2015
Don't pay for a vacation to nowhere - March 19, 2015
It's the IRS calling…or is it? - March 12, 2015
Cleaning up without getting cleaned out - March 6, 2015

10. When shopping online be careful and look for boxes that are pre-checked for you to receive offers from them or their partners. Be sure to **uncheck the boxes** and **opt-out** if you don't want to receive any communications. Even legitimate retailers count on you not unchecking the boxes to opt-out.

The Illustrated iTunes License Agreement

----

   by Michael E. Cohen:
<mcohen@tidbits.com>, @lymond
   article link:
<http://tidbits.com/e/16056>

   If you have ever bought anything from the iTunes store, you have surely seen it before — at least the first couple of paragraphs if you haven't bothered to scroll down in the dialog: the iTunes Terms and Conditions to which you have to agree before you can buy anything. It's not the most gripping prose you'll ever encounter, but artist R. Sikoryak nonetheless found it inspiring enough to make it into a graphic novel, "iTunes Terms and Conditions: The Graphic Novel."

<http://itunestandc.tumblr.com/>

   Currently comprising (as of this writing) 54 multiple panel pages drawn in the style of a variety of artists that includes Edward Gorey, Chester ("Dick Tracy") Gould, Kate "Hark! A Vagrant") Beaton, Hank ("Dennis the Menace") Ketcham, and Rube Goldberg, the terms and conditions appear as the narrative text for an ongoing action adventure story starring Steve Jobs (among others) in a variety of guises. The story begins at the very bottom of the Web page, so scroll all the way to the bottom and start reading to find out what you have agreed to as you attempt to unravel the story behind the story.

<http://www.harkavagrant.com/>
<http://tidbits.com/resources/2015-11/pg-41-rube-goldberg.jpg>

   ----

   read/post comments:
<http://tidbits.com/e/16056#comments>
   tweet this article:
<http://tidbits.com/t/16056>

   iOS 9: TidBITS Answers Your Questions

   <http://tidbits.com/e/15931>

Have iOS 9 questions? We've got answers! And if you come up with more questions, ask them in the comments, and we'll do our best to update the article with what you need to know.

How to See Your iPhone's Precise Signal Strength

----

by Josh Centers:
<josh@tidbits.com>, @jcenters
article link:
<http://tidbits.com/e/15856>
6 comments

For decades, cellphone owners have relied on signal bars to determine the strength of the cellular signal. Since iOS 7, iPhone (and cellular iPad) users have become accustomed to signal dots, which do the same thing. But neither is a precise indicator, and you can't necessarily predict what will or will not be possible when a particular number of dots are lit up.

Cellular reception in my area is awful, especially in my house. Sometimes voice calls work OK with one dot, but fail at three dots. Cellular data is even more unpredictable. My iPhone's Internet connection often doesn't work at all unless I have LTE coverage; 3G is almost as bad as no signal at all these days.

The folks over at Tech Insider have produced a video that will help you see what your signal strength is numerically, for troubleshooting purposes. But for some reason, they didn't also write up the instructions for those who prefer reading. So if you fall in that camp, here's how to see your iPhone's precise signal strength:

<http://www.techinsider.io/iphone-signal-reception-carriers-strong-field-test-2015-8>

1. Open the Phone app

2. Dial *3001#12345#* and tap the green call button to put your iPhone into a secret Field Test Mode

<http://tidbits.com/resources/2015-08/Field-Test-Mode.png>

3. Hold the Sleep/Wake button until the Slide to Power Off screen appears

4. Release the Sleep/Wake button and ignore the Slide to Power Off prompt

5. Hold the Home button until you go back to the Home screen

Instead of dots, you should now see a negative number in the upper left, like -102. This is your exact signal strength, measured in decibels, called the Received Signal Strength Indication (or RSSI if you want to impress technical support). The higher the number, the better, but note that these are negative numbers, so -1 would be an out-

standing signal, while -1000 would be beyond poor. In the real world, you'll probably see signal strengths somewhere between -40 (a five-bar signal) and -120 (a one-bar signal).

What if you get tired of trying to interpret the numbers? Tap the numbers to switch back to dots; another tap brings the numbers back again. And if you want to go back to dots permanently? First, restart your iPhone by holding the Sleep/Wake button, swiping the Slide to Power Off Switch to the right, and then pressing the Sleep/Wake button again to turn it back on. Then, to get rid of the numbers for good, go back into Field Test Mode and exit it by pressing the Home button.

I've been arguing with Verizon Wireless for years about my poor service, and have consistently received the runaround. The closest I've come to receiving actual help was being told to dial ### after a dropped call to mark it in Verizon's records. (Give that a try the next time you lose a call!) But since standard cellular voice calls drop so consistently, I usually use Google Hangouts or FaceTime instead, and thus never have an opportunity to report problems. Sigh…

Now I can go to Verizon with this new, accurate information, and maybe someone technically minded will take me seriously. I'm not going to hold my breath.

----
read/post comments: <http://tidbits.com/e/15856#comments>
tweet this article: <http://tidbits.com/t/15856>

◆━━━━━━━━━━━━━━━━━━━━◆

What To Do If Your iPad/iPhone Is Taken

By Bill Crowe, 2nd Vice President, Sarasota
PCUG, FL
January 2014 issue, PC Monitor
www.spcug.org
editor (at) spcug.org

Last month I wrote about how to secure your device. This month is about what to do if a bad guy got your device. There are several things that can be done:

If you enabled Find My iPhone on your missing device
To enable find my iPad/iPhone
1. Enable iCloud by going to Settings>iCloud, and entering your Apple ID and Apple passcode(password)
2. Turn on Find My iPad

These steps are can be followed if Find My iPhone/iPad was enabled on your device *before* it was lost or stolen.
1. Attempt to locate your device using Find My iPhone at icloud.com/find, or using the free Find My iPhone app.
2. Put the device in Lost Mode to set a 4-digit passcode and display a custom message with your phone number on your device. While the device is in Lost Mode, you can also keep track of changes to your device's location. Lost Mode requires that your missing device be using iOS 6 or later. If your device is using iOS 5, you can still lock your device remotely and display a message on the screen.

Use lost mode or lock a device:
- Sign in to icloud.com/#find with your Apple ID (the one you use with iCloud) If you're already using an iCloud web app, click the app's name to switch apps.

- Click All Devices, then select the device you want to track or lock.
- Click Lost Mode (iOS 6 or later), or Lock (iOS 5 or OS X v10.7.5 or later).
- Follow the onscreen instructions, keeping the following in mind:

  - If your iOS device already has a passcode, that passcode is used to lock the device.
  If you're asked to enter a passcode, that passcode will be required to unlock the device.
  If you're asked to enter a phone number, enter a number where you can be reached. The number appears on the device's locked screen.
  If you're asked to enter a message, you may want to indicate that the device is lost or how to contact you. The message appears on the device's locked screen.
  If your device is online, it locks and tracking begins (if applicable). If Location Services is turned off on the device, it's temporarily turned on to track its location. A confirmation email is sent to your Apple ID email address.
  If it's offline, the lock and tracking (if applicable) take effect the next time it's online.
  - If you used Lost Mode, you see the device's current location, as well as any changes in its location on the map.

To change the message or phone number shown on the lost device, or to turn off Lost Mode, click Lost Mode, then make your changes.
- o Note: If you forget the passcode, then lock it and later find it, you may need to take it to an authorized repair center to unlock

3. If you want to delete all of your personal information from your missing device, you can [erase it remotely](). Please note that when you erase a device, you will no longer be able to locate it.
4. Report your lost or stolen device to local law enforcement and your wireless carrier. Apple doesn't track or flag lost or stolen products, but you can use My Support Profile ([supportprofile.apple.com]()) to find a list of serial numbers for products that you've purchased or registered with your Apple ID.

Note: If your missing device is offline, you can still put it in Lost Mode, lock it, or erase it. Your commands will take effect when the device comes back online.

If you did not enable Find My iPhone on your missing device
If you did not enable Find My iPhone before it was lost or stolen, you can't use it to locate or protect your device, but you can still follow these steps:
1. [Change your iCloud password]() to ensure that no one else can use your device to delete or make changes to your iCloud data.
2. Report your lost or stolen device to local law enforcement and your wireless carrier. Apple doesn't track or flag lost or stolen products, but you can use My Support Profile

([supportprofile.apple.com]()) to find a list of serial numbers for products that you've purchased or registered with your Apple ID.

Officers & SIG Leaders

Leader: _____George Carbonell   568–0492   george.carbonell@comcast.net
Secretary: _____Stuart Rabinowitz
Treasurer: _____Charles Gagliardi   233–0370   epencil@aol.com
Director at Large: __Phil Manaker   659-4584   amanaker@earthlink.net
Director at Large: __Ted Bade   643-0430   tbade@cox.net
Director at Large: __Stuart Rabinowitz   633–9038   s.e.rabinowitz@att.net
Web Manager: _____Bob Bonato   bob@bonatodesign.com
Membership: _____Richard Sztaba   richer1@aol.com
Integrated SIG: ____Stuart Rabinowitz

December, 2015

		1	2 **1977 ARC (1st LAN) announced**	3	4	5
6	7	8	9 **1968 Englebart mouse demo**	10 **1815 Ada Lovelace born**	11	12
13	14	15 **General Meeting 7 PM**	16	17	18	19
20	21	22	23	24	25	26 **1791 Charles Babbage born**
27	18	29	30	31		