The Rochester Computer Society, Inc.
a computer club for everyone
Founded 1982

MONITOR

Vol. 32, No. 9 September 2015

Next Meeting
Tuesday, September 8

Nick Francesco!

Contents

Will YOU Pay the Netflix Tax?

by Bob Rankin
askbobrankin.com

This month, the City of Chicago extended its 9% "amusement tax" to include "electronically delivered amusements" such as Netflix, Amazon Prime, and even pay-per-view cable TV programs. And these new taxes could be headed to your city next. Here's what you need to know.

Can Local Governments Tax Cloud Services?

Do you subscribe to Netflix, Spotify, or Pandora? How about Amazon Prime, iTunes, HBO Go or Hulu? Do you enjoy online gaming via Xbox Live, PlayStation Network, Gamefly, or Google Play? If you answered yes to any of those, you could be paying more for them soon.

In addition to the new taxes on consumer "amusement" services, Chicago simultaneously expanded its unique 9% tax on business property lease payments to include "nonpossessory

computer leases."

That includes Amazon Web Services, Microsoft Office 365, MLS real estate listings, Google Apps for Business and just about any cloud-based business service used from a computer in Chicago. Adding irony to the insult, if you're a Chicago-based law firm and subscribe to LexisNexis or WestLaw online, that means you'll be taxed just for reading the list of new taxes.

Netflix Tax

City officials are claiming this is not a new tax, but simply a "clarification" of long-standing use tax policies. Right…. The effect is that an $8.99/month Netflix subscription will now cost Chicagoans $9.80/month. That example may be trivial, but Chicago's tax authorities estimate the "clarified" rules will generate an extra $12 million per year in revenues.

Oddly, the amusement tax is applicable only to streaming services; it does not apply to music or video files purchased outright and downloaded to a Chicagoan's hard drive. (Purchases are subject to state and local sales taxes.)

Odder still is Netflix's instant capitulation to the Chicago tax rulings. The company says it's already working on a way to tack the extra 9% onto its Chicago users' monthly bills. Other streaming entertainment providers have yet to weigh in on this issue. You'd think Netflix might, for the benefit of their subscribers, at least put up a little fuss. But no.

Less Legalese, Please!

The "nonpossessory computer lease" tax applies to just about any subscription to a searchable Web site. The key is whether the consumer's control over the remote computer is more than "de minimis," or negligible. In its new rules, the Chicago tax authority compared a passive stock price feed (which may require a subscription) to a searchable database of real estate listings. The stock price feed would not be taxed but the database subscription would be taxed.

The rules don't specifically address non-subscription payments for use of remote computing resources. But Chicago's tortured interpretation of a taxable "lease" could easily encompass one's monthly eBay, Etsy, or other ecommerce platform bills.

That's the point, of course. Chicago, like every other municipality, has watched its brick-and-mortar tax base erode over the years. Expanding old sales and use tax laws to encompass new, Internet-based modes of commerce is one way to recoup those lost revenues. And if Chicago gets away with it, other municipalities will certainly follow.

But *can* Chicago get away with this? Legally, the city (and, by extension, all cities) seems to be on shaky ground, according to Catherine A. Battin, a partner in the Chicago office of law firm McDermott Will & Emery LLP; she writes:

"(I)t is questionable whether Chicago can impose tax on the deemed use of hardware and software physically located outside of its jurisdiction, particularly when the control over the hardware and software is so attenuated. Moreover, the tax can be challenged on the grounds that such an imposition of tax exceeds the City's home rule powers, violates the Uniformity Clause of the Illinois Constitution, the Internet Tax Freedom Act, and the Commerce Clause of the United States Constitution … a challenge to the tax by a taxpayer or a coalition of taxpayers is imminent."

Just Put it Back in the Mailbox

It's pretty easy for some to evade this tax. Chicago relies on a user's billing address to determine if he/she is "in Chicago" for the tax's purposes. So a multi-location law firm, like Battin's, can simply pay its Lexis-Nexis bill from a non-Chicago location. Netflix users can shift their billing address to an out-of-Chicago friend or family member. But it would be impossible or impractical to do the same for Amazon Prime and all your other online accounts, just to save

a few dollars a year.

Finally, this tax is due from users, not providers. Such "use taxes" are notoriously difficult to collect because users simply don't report themselves voluntarily. Obvious big targets, such as law firms and software developers, will see greater scrutiny from Chicago's tax auditors. But without the cooperation that Netflix has inexplicably offered, I don't see Chicago and like-minded municipalities successfully collecting these taxes from many consumers and small businesses.

Do I Need the Facebook App?

Q. I use Facebook in a browser on my Android phone. I don't understand why, if I can easily use it in a browser, do I need to install the Facebook app?

A. Excellent question! You certainly can continue to use Facebook as you are doing and it will continue to work pretty much as it normally does. But some things won't work. Anything that requires Flash, for example, is not supported in an Android browser. If it requires Flash to run, most developers have created an app to make it work.

So do you have to use the Facebook app? No, but keep in mind that not all features will work in a browser version. The app version is specifically designed to work on your device.

Q. I am using Windows 7 and Vista and I would like to know where the Scan Disk and the Defragment options are. Can you help, Mr. M?

A. The location of these features is the same in both Vista and Windows 7: Click Start > Computer, then right-click the drive you want to check and select Properties. Click the Tools tab, then the Check Now button which appears under Error Checking. That will bring up the Check Disk window where you can then select whatever options you want to use.

Q. I use the Yahoo! Address Book. When I click the Contacts tab, I can view all my contacts, but I can't find how to get into my group categories to edit them. The only choices are Add Contact, Add Category and Tools, but nothing about editing. Any suggestions?

A. To edit contact information in your address book, click to select a contact, then click the Edit link to the right of the contact you want to change. Make the necessary changes and click the Save button.

Q. How do you change the default font in Word 2007?

A. Simply open a new Word document. If you are already in Word, click the Microsoft Office Button at the top left of the screen, go to the New Document pane, click New, then Blank Document.

Click Font in the Font group and choose the font style and point size that you want to use as your default. Click Default and a dialog box will open and ask if you want to make the change to all new documents based on the Normal template, so click OK.

Q. I have 254 addresses in my Gmail contacts list. How can I transfer these into six established groups without the painful process of copying each address onto paper and then retyping them into their respective areas? Thank you for your help.

A. Display your Contacts in Gmail, then click to select individual contacts. With the list of Groups displayed, select the Group you want to move the selected contacts into. They will pop

right into the selected group.

If you need additional assistance, go into your Gmail Help by clicking the little menu icon to the far right of the Address field, select Help. Search for "Groups" and you will find detailed instructions and group information.

Mr. Modem's DME (Don't Miss 'em) Sites of the Month

Death To Stock Photos

If you would like to receive free, high- quality photos in your Inbox every month, have I got a site for you! Register and not only will you get images sent directly to your Inbox each month, but you will also receive a free pack of photos for signing up. Visit the Web site to view a healthy sampling of quality images. The sign-up field is prominently displayed, or you can scroll down the page to learn more, view photos and check out the licensing terms.
http://deathtothestockphoto.com

ePinions

Before you buy a product, look it up on ePinions, a Web site that compiles the opinions and experiences (good, bad, or ? Are you kidding me?) of real-life consumers about all sorts of products and services. It's also excellent for comparison shopping. ePinions covers millions of products and services in a variety of categories. In addition to detailed product reviews, you can read buying guides ("What should I consider when buying a pit bull"?) and "how-to" guides ("How do I perform my own appendectomy") Once ePinions helps you decide what you want to purchase, you will find pricing and availability options through a list of rated online merchants. Another excellent site featuring ?real people, real reviews? is Yelp.com.
www.epinions.com

NationMaster

If you like useless but interesting, facts and numbers, then you will probably enjoy this site which hosts statistics from the CIA World Factbook (http://tinyurl.com/2h2e3k). Type a topic into the text box at the top of the page and click Search to see a list of statistics, encyclopedia entries and more. The default font is fairly small, so with most browsers, press CTRL and the + sign to increase font size, or View > Zoom.
www.nationmaster.com

To subscribe to Mr. Modem's award-winning weekly computer-help newsletter and also receive personal responses to your questions, visit www.MrModem.com.

Should You Get a Laplet?

by Bob Rankin
askbobrankin.com

When it comes to computers, there are more choices than ever before: desktop PCs, laptops/notebooks, tablets, "phablets" which fall somewhere between a smartphone and tablet, and "laplets" – a cross between a laptop and a tablet. Let's take a look at the wonderful world of laplets…

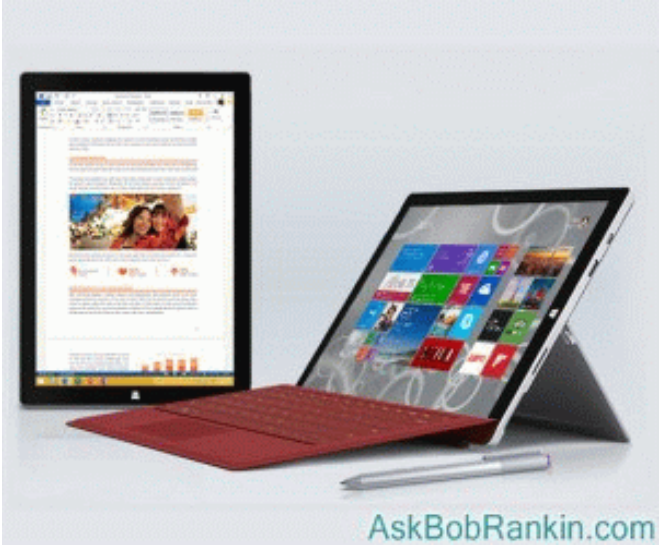
What is a Laplet?

A laplet combines the portability of a tablet with the processing power and productivity features of a laptop. The "guts" of the device reside in the display's chassis; when you want to travel fast and light, just detach the display from the keyboard and take your tablet on the road. A tablet is great for movies, music, and Web browsing.

But when you need to sit down and work seriously for a while, you need that keyboard. When you need to plug in speakers, a printer, a wireless mouse, and other peripherals, you

need the plethora of ports that a laptop provides. Then you just reunite a laplet's display and keyboard, et voila' – laptop mode!

A laplet is similar to an Ultrabook in terms of light weight, long battery life, and thinness. Laplets generally contain more powerful CPUs, such as an Intel Core i5, more RAM, and more storage space than tablets. Laplets come with touchscreens, like tablets, as well as keyboards.



What is a laplet?

Microsoft Windows 8.1 and 10 are the only operating systems pre-installed on laplets at this time. Apple's OS X does not support touchscreen features, or the laplet concept. Some Linux distributions support touchscreens, but you won't find them in the aisles of Best Buy.

Microsoft's Surface Pro 3 is probably the best-known laplet. Introduced in May, 2014, it runs 64-bit Windows and features a 12-inch touch screen with 2160x1440 pixels; it also supports up to three external displays. Intel i3 dual-core CPU options range from 1.5 GHz to 3.3 GHz. RAM capacity is either 4 GB or 8 GB, and SSD storage ranges from 64 GB to 512 GB. Battery life is up to 9 hours. The Surface Pro tablet alone weighs only 1.76 pounds.

The price is a bit heavier. Surface Pro starts at about $800 and quickly soars to nearly $2,000 with maximum clock speed, RAM, and storage. Even at the high end, you still don't have a keyboard. That costs an additional $130. A docking station that supports multiple video inputs, Ethernet, and five USB ports will run $100 to $150.

More Laplets to Consider

Apple CEO Tim Cook derisively likened the laplet to "crossing a toaster with a refrigerator." But Apple CEOs aren't always right about what tech gadgets people want. When 7-inch tablets first arrived, Steve Jobs said "7-inch tablets are too big to compete with a smartphone and too small to compete with the iPad ... 7-inch tablets are going to be dead on arrival." He also reportedly said that users would "have to sand down their fingers" to use such a small tablet properly. When 7-inch tablets proved to be popular, Apple came out with their own, the iPad Mini.

Lenovo's Yoga 3 Pro upstages the Surface Pro in style, size, and price. But reviewers have been disappointed by the new Intel Core M processor's performance. Starting at $950, the Yoga 3 Pro features a 13.3 inch screen and an ultrathin/ultralight design.

The ASUS Transformer Book is a lot more affordable – about $250 street price. But it has a dinky 10.1 inch screen and commensurately cramped keyboard, only 1 GB of RAM, and just 32 GB of storage. A year's worth of ASUS WebStorage is included. The Intel Atom CPU runs at 1.83 GHz but is less powerful than the dual-core i3. Bluetooth 4.0 allows wireless connection of compatible peripherals.

Acer's Aspire Switch 10 E laplet packs a bit more performance than the Transformer Book, with 2 GB of RAM and 64 GB of storage. The Switch also includes a 500 GB hard drive in the detachable keyboard-base. Refurbished units are going for about $200 at Newegg.

Laplets make sense for students, travelers, and other on-the-go users. As prices continue

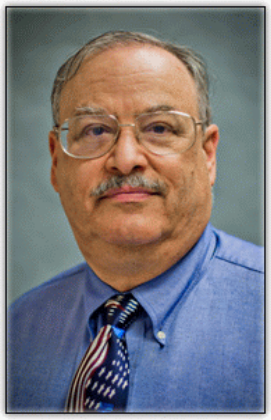
to fall, we should see more laplets replacing separate laptops and tablets. But there will always be trade-offs in a converged product; smaller keyboards and less versatility versus portability and battery life.

Courtesy of Mr. Rankin.

Security Bug Could Threaten 950 Million Android Devices

by Ira Wilsker

In recent weeks, at least two potentially frightening new vulnerabilities have been discovered that could threaten an estimated 95 percent of the one billion devices running the Android operating system. The good news is that as of this writing, there have been no documented attacks on Android devices that take advantage of these two security vulnerabilities. The bad news is that now that information on these security vulnerabilities has been widely published, as well as presented at the recent Black Hat hacker and security convention in Las Vegas, it may only be a matter of time until some bad guys start to take advantage of these security vulnerabilities.



Google, the progenitor of Android, was promptly made aware of the vulnerabilities as soon as they were uncovered, and has produced patches and fixes for many of the Android devices that have these vulnerabilities. The problems is that with the exception of a few models of Nexus smart phones supported directly by Google, it is up to the phone manufacturers or the cell phone carriers to release the upgrades and patches to close these vulnerabilities. At present, none of the major third party security software publishers provide any protection, leaving many of us vulnerable.

One of these newly discovered Android vulnerabilities was given the moniker "Stagefright" by its finder, Joshua Drake, vice president of platform research and exploitation at Zimperium. Drake first reported on the Stagefright vulnerability in April, disclosing his findings to Google, which quickly developed and provided security patches to its Android partners. Most of these Google partners who have not yet provided the patches to their respective customers may not do so for months, if at all; many phone manufacturers and carriers have explicitly stopped supporting and patching older Android phones, which are still in use by the millions. In several media interviews, as well as his Black Hat presentation, Drake explained that, "All devices should be assumed to be vulnerable." As stated in a July 27 Forbes magazine interview, Drake said that he believes that as many as 950 million of the one billion Android phones currently in use may be vulnerable to the Stagefright vulnerability. Drake went on to say that only older Android phones running versions of Android below version 2.2 will not be potentially affected by this bug.

It is important for Android users to understand that Stagefright is not a virus or other form of malware that could infect a phone, but is instead a bug, or unexpected and unforeseen security vulnerability in the Android software itself. This vulnerability is in the heart of the Android software that processes, plays and records multimedia files.

According to Drake, the security vulnerability may allow a hacker to illicitly access the targeted device by simply sending an MMS message (text message) or multimedia file. What is especially nefarious about the Stagefright vulnerability is that it can be taken advantage of by a hacker without any action by the user; the victim does not have to open or click on anything in order for the hacker to access a device. It is also theoretically possible for a hacker to capitalize on this vulnerability when an unsuspecting victim opens a purloined video file on

a website. Once a hacker has taken advantage of this security gap in Android, he can access the victim's camera, microphone, and any data or images in the device's external storage. On some devices the hacker can also gain root access to the inner workings of the device.

In order to easily determine if a particular Android device is vulnerable to the Stagefright vulnerability, Zimperium has released a free "Stagefright Detector App" available from the Google Play Store. A similar detector utility was just released by the security software company Lookout, which it simply calls "Stagefright Detector." While these utilities will detect the vulnerability, it will still require a patch or other fix from the phone maker or the cell phone carrier supporting and updating the device.

When I first read of this Stagefright vulnerability and the availability of the detector, I downloaded and installed the detector. My year old Huawei Ascend Mate 2 phone, which had previously been upgraded by Huawei to Android Lollipop 5.1 (from 4.4), had the Stagefright vulnerability; coincidently, just yesterday (the day before typing this column), I received a patch from Huawei that, among other benefits, closed the Stagefright vulnerability on my phone. I reran the Stagefright detector from Zimperium to confirm the fix, and the vulnerability on my phone has definitely been patched by the recent update.

Another Android security vulnerability was disclosed at the recent Black Hat security convention. Well-known security company Check Mate disclosed this newly recognized bug, which it named "Certifi-Gate," which may potentially allow a hacker to take control of a victim's phone by utilizing the "Remote Support Tools (RSTs)" software that was installed on the phones by the manufacturers, often at the behest of the cell phone carriers selling those particular phones. Check Mate promptly notified the device makers and cell phone companies of the vulnerability.

According to Check Mate, there are millions of phones and tablets made by Samsung, ZTE, HTC, LG and other manufacturers that have incorporated this vulnerable "remote support" function software on their phones; according to Google, Nexus phones do not have this particular vulnerability. Using a security method known as digital certificates, hackers can spoof or counterfeit these supposedly secure digital certificates, allowing them the same access to the internals and functions of the phone that had previously only been allowed to legitimate support personnel. Once the hacker has tricked the phone or tablet into accepting a spurious digital security certificates, he or she now has direct access to personal information stored on the phone and can turn on the microphone to remotely record conversations, track the location of the device and its user, and otherwise threaten the security and privacy of the victim.

While the device manufacturers and cell phone carriers were promptly notified of the vulnerability, it may be months, if ever, before they push the patches to this newly discovered vulnerability. Users can download a free utility that will show the user if a device is vulnerable to this remote support vulnerability. Written by Check Mate, the utility "Certifi-Gate Scanner" can be downloaded directly from the Google Play Store.

According to Check Mate, in order for hackers to take advantage of this vulnerability, the user must first download and install an application that contains the code that gives the hacker the access. The Google Play Store continuously monitors the apps that it makes available, checking them to make sure that they do not contain any malware. Check Mate advises that users to install applications from a trusted source, such as Google Play."

With the continual battles among users who seem to love arguing iOS and iPhones versus Android devices, iPhone users should not gloat over these Android vulnerabilities. At the Black Hat convention in 2013, which is where many hackers and crackers rub shoulders with security experts, the vulnerabilities of iOS devices, specifically iPhones, was discussed. In one of the presentations, despite the false but widely held belief that iPhones are immune to attack

and are very secure by nature, researchers from the Georgia Institute of Technology were able to inject persistent, undetectable malware into iPhones, iPads and other iOS devices using the latest generation of the iOS operating system. Using a modified USB charger, nicknamed "Mactans" after a type of black widow spider, the researchers were able to compromise any current generation Apple device in under a minute.

Check your smart phone for these vulnerabilities, and do not download apps from any source other than reputable sources such as the Google Play Store or the Amazon App Store. Do not open any text messages from people that you do not recognize, although text messages can be spoofed just as e-mails are frequently spoofed. If you find that your device maker or phone carrier is providing a patch, update, or upgrade, strongly consider taking advantage of the offer and update your device immediately.

More Security Vulnerabilities Disclosed for Phones, Carriers

by Ira Wilsker

If you are like me, I carry my cell phone everywhere, carrying on voice conversations, sending and receiving text messages, utilizing countless apps, and surfing the Web. Until recently, I gave very little heed to the security of these external communications as our smart devices are supposed to be somewhat secure. GSM carriers like AT&T and T-Mobile utilize encryption to make communications secure; CDMA carriers like Sprint and Verizon also claim to have secure networks. Yes, I do have a major security app on my Android phone that scans new apps and text messages for malware, as well as protects from hazardous websites. Google created Android to be secure, with apps running in a somewhat closed memory space, called by some a "sandbox," which is supposed to prevent purloined apps from talking over the phone. iPhone fanatics, along with many Apple fans in general, believe that their devices are immune to attack, as Apple would not dare to allow any threats to harm their beloved devices.

Now welcome to the world of stark reality. In a recent column, I wrote about two newly revealed vulnerabilities, known as "Stagefright" and "Certifigate," that may threaten the security, safety and privacy of nearly a billion smart phones and tablets. Since then, others have come forward demonstrating previously unannounced security vulnerabilities that threaten the security of our smart phones, often including both iPhones and Android devices in their threat assessments.

One of these newly disclosed threats explicitly targets the most tech-nology innocent and un-informed among us. Ap-propriately called "grandma malware," this clever piece of malware sneaks onto Granny's phone using a compound method of infection designed to defeat many of the simplest security precautions. While recently updated Web browsers and desktop security software, as well as updated phone operating systems, have likely patched the vulnerabilities, Granny's often older and unpatched computer and phone may be vulnerable. The first step in the infection se-quence occurs when the victim downloads an innocent looking app, often a game or simple photo utility, onto their computer using any one of the older versions of most of the common Internet browsers, which are still in wide use. This small utility, explicitly designed to appeal to a "grandma," does not itself contain any malware, and will pass the scrutiny of many of the less sophisticated desktop security products. This utility sits quietly and apparently innocently on the victim's computer, often performing its intended tasks. The app surreptitiously monitors Web surfing until Granny logs on to an app store, such as the Google Play Store. The malicious utility captures the logon and connection information from the app store; with this information, the malware is invisibly downloaded wirelessly to the smart device, installing itself on Granny's phone. Once installed, this malicious app immediately gathers personal data from the phone and sends it to parties unknown. Even if

this malware is detected and removed in a subsequent security scan by a third party security utility, it is too late; all of the personal information was stolen within seconds of the app being installed on granny's phone. Granny's private information has just been stolen, and she might very well become an identity theft victim; as is common in criminal enterprises, the most vulnerable among us are more likely to be victimized.

Despite the travesty of purposely going after Granny, it is not one of the most insidious of the newly announced threats imperiling our smart phone usage. In recent days, a pair of IBM cyber security analysts, Or Peles and Roee Hay, uncovered a flaw in the Android operating system still being used in over a half-billion Android smart phones. This vulnerability, not yet formally named but referred to as a type of "masque" attack, could allow hackers to take over and remotely control vulnerable Android phones. According to these researchers, "Masque attacks are defined as malicious apps uploaded, say, from e-mails directing victims to fake Web links." According to Peles and Roee, Google has issued patches for devices running Android 5.1, 5.0, 4.4, and Android M, but as often the case for many Android devices (except some Nexus phones), it is up to the phone manufacturer or cell phone carrier to push these patches to their users, meaning that although the patches are available, over half of Android phones do not yet have the patches installed.

This "masque" attack vulnerability allows hackers to control the security privileges that are a part of the Android operating system, allowing compromised or counterfeit apps to access information on the phone that would otherwise be unavailable to the hacker. According to the researchers, this vulnerability allows the data thieves to steal personal information, capture banking information including logins and passwords, access the phone's cameras, download contact lists, and pilfer stored files and e-mails, sending the stolen information to a remote server. While this particular Android vulnerability was recently discovered by IBM cyber security experts, it is very similar to one discovered several months ago by FireEye that explicitly targets Apple's iPhones. The mechanism and modus operandi, as well as the data thefts, are almost identical between the Android and iPhone vulnerabilities.

A "masque" attack can occur when smart phone users download any of 11 authentic looking but counterfeit or contaminated apps that also appear to work properly when downloaded and installed. Among the most commonly downloaded iPhone and Android apps that enable this vulnerability are modified copies of Facebook, Twitter and WhatsApp. According to FireEye, iPhones are as vulnerable to these masque attacks as Android devices. According to Zhaofeng Chen, a senior research engineer and scientist at FireEye, the 10 tainted apps that most threaten Apple devices are "WhatsApp, Twitter, Facebook, Facebook Messenger, Google Chrome, Blackberry Messenger, Skype, WeChat, Viber, Telegram and VK." These apps are

often downloaded from genuine-appearing links in e-mails or SMS text messages, and mimic the functionality of the genuine app, but allow for the remote access to this valuable personal content. FireEye was quoted as stating that this iPhone vulnerability can steal or access a variety of information from compromised phones. Among the dastardly deeds that this masque vulnerability can perform include recording and forwarding phone calls placed on Skype, Wechat and other voice apps; intercept text and SMS messages from iMessage, WhatsApp, Facebook Messenger, Skype and other SMS apps; send real-time and historical GPS locations; access website histories; steal contact information and lists; and download photos from the phone. Apple has created patches and upgrades closing this vulnerability, and pushed these patches to many of its users, but there are inevitably iOS device users who have not received or installed these patches.

In recent days, on the Australian version of the "60 Minutes" news magazine, another cell phone vulnerability was demonstrated where hackers in Germany were easily able to listen in on a cell phone chat between individuals in Australia and the UK. This ability to readily capture live calls is known as the "SS7 Vulnerability." SS7 technology is widely used, legitimate and necessary for cell phone carriers to properly direct calls and text messages to their intended recipients. ComputerWeekly .com said, "Like any protocol, SS7 is vulnerable to exploitation by sophisticated and well- funded third parties with criminal intentions." In another ComputerWeekly.com story titled "Security flaw exposes billions of mobile phone users to eavesdropping," the online magazine says, "Hackers, fraudsters, rogue governments and unscrupulous commercial operators are exploiting flaws in the architecture of the mobile phone signaling system known as SS7. ... Billions of mobile phone users around the world are at risk from covert theft of data, interception of their voice calls and tracking of their location." SS7 is not a vulnerability in the phones themselves, as the vulnerability is not brand or operating system dependent, impacting Android, iPhone, Blackberry and other systems equally, but is in reality a vulnerability in the switching system utilized by the cell carriers themselves.

For those of us who routinely use Android, iOS or Blackberry devices without much thought about the inherent security vulnerabilities of the phones and cellular carriers, keep at least a spark of consideration in mind. While I am fully cognizant of the risks, I will continue to use my smart devices pretty much as I have in the past.

Websites:

http://www.foxbusiness.com/technology/2015/08/14/new-cyber-hacks-for-mobile-hacks-discovered/
http://www.komando.com/happening-now/320997/watch-out-for-grandma-malware
http://www.dailymail.co.uk/news/article-3199978/Hackers-access-call-message-send-world-moment-German-computer-experts-just-easy-eavesdrop-smartphone.html
http://www.computerweekly.com/news/4500251809/Mobile-phone-users-at-risk-as-hackers-bug-and-track-victims
http://securityaffairs.co/wordpress/22605/hacking/fireeye-discovered-apple-vulnerability-allows-ios-keylogging.html
http://www.computerweekly.com/news/4500251756/Security-flaw-exposes-billions-of-mobile-phone-users-to-eavesdropping
http://media.ccc.de/browse/congress/2014/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel.html#video
https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html
http://www.reuters.com/article/2014/11/10/us-apple-cybersecurity-idUSKCN0IU1W620141110

Courtesy of Mr. Wilsker.

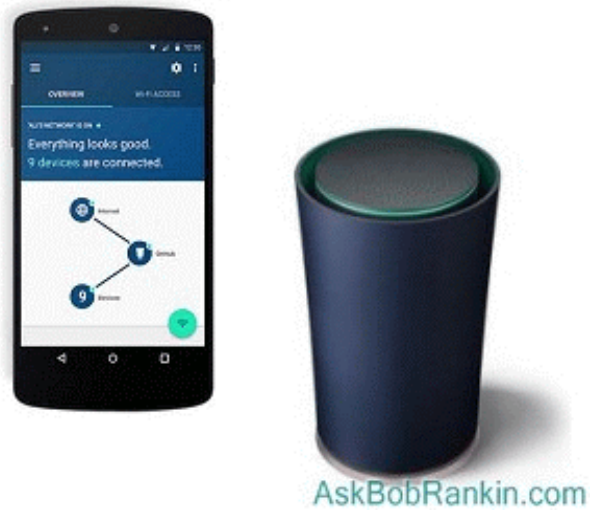
Google OnHub: The Ultimate WiFi Router?

by Bob Rankin
askbobrankin.com

Google entered the WiFi router market in August 2015, with a mind-boggling product called "OnHub." It doesn't look anything like a traditional router, and it doesn't act like one either. And that's a good thing! Read on to learn more about this router, and why you're going to want one...

What is OnHub?

OnHub does not behave the way people expect a router to behave, either. It's actually consumer-friendly! Built by Google hardware partner, TP-Link, OnHub is easy to set up, highly reliable, and maintenance-free. It's also packed with features that many of us have long desired. (It also looks remarkably like Amazon's Echo tabletop personal assistant. More on that later...)



For example, OnHub's built-in network monitor shows you all devices on your WiFi network and how much bandwidth each device is using – in real time, on your Android-powered mobile device! The OnHub app provides tap-button control over bandwidth prioritization. That means Junior's gaming won't make Mom and Dad's Netflix movie all jittery, or vice versa if it's the kids' turn to hog the Internet.

OnHub has 13 internal antennas (that is not a typo) configured in concentric rings, to deliver maximum signal coverage consistently over wider areas. During setup, for which the Android app is required, OnHub automatically scans all available channels and selects the best overall signal on either 2.5 GHz or 5.0 GHz radio frequency bands. Supported protocols include 802.11 a/b/g/n on 2.5 bands; 802.11 a/n/ac on 5.0 GHz; an auxiliary 802.11 a/b/g/n/ac radio. There's a 10/100/1000 Mbps Ethernet port and switch.

Google OnHub Wifi Router

WiFi connections are secured with WPA2-PSK encryption. Another cool feature of the OnHub app is easy password-sharing. If you want to let someone share your WiFi, just tap on his/her device displayed in the app and the device gets your network's password until you revoke that privilege. There's no need for the guest to know your password, and no need to change every "resident" device's password after the guest leaves.

Configuring and managing a WiFi network via a wireless Android app is inherently less secure than the traditional requirement for a hardwire Ethernet connection to the administrator's console built into a router. But Apple's Airport Express routers have used an iOS app in the same way without major problems. Speaking of Airport Express, its $200 price tag is identical to OnHub's. The Airport is also tall to accommodate multiple antennas; but with its flat sides and rounded corners it looks like a piece of Tupperware for keeping saltine crackers fresh. The OnHub is definitely more stylish.

No More Blinking Lights

Instead of tiny blinking lights, OnHub displays its status with six tri-color LED arrays

arranged in rings around the chassis. Your router's status is clearly viewable from any angle. An ambient light sensor keeps the LEDs from shining too brightly or being washed out in sunlight. You can also view the status of the OnHub, and manage the connected devices via an app for your mobile phone.

OnHub won't become obsolete in 3-5 years, as many older routers have. In fact, it already has future protocols built into it, including proposed home-automation protocols Bluetooth Smart, Google Brillo/Weave, and IEEE 802.15.4. OnHub has 4 GB of internal flash memory, ample room for future upgrades and new features. Of course, OnHub automatically receives software updates from Google, just as the Chrome browser does. You don't have to worry about doing manual firmware updates.

There's a bit of mystery surrounding two details of OnHub. Google isn't saying what the USB port is for, or what you might hear from the 3-watt speaker mounted atop the OnHub. My guess is that OnHub's resemblance to Amazon's Echo is no accident; you're going to talk to OnHub and it will talk back, someday soon.

One thing I've worried about when considering a replacement for my router is whether it will work with my Verizon FIOS service. But the OnHub website promises that "It works with cable, DSL, Fiber, and all major Internet service providers."

The only bad thing about OnHub is that you can't get one today. But at the top-right corner of every OnHub Website page is a "pre-order" button that you can click to get in line. Google says OnHub will be shipping "in coming weeks."

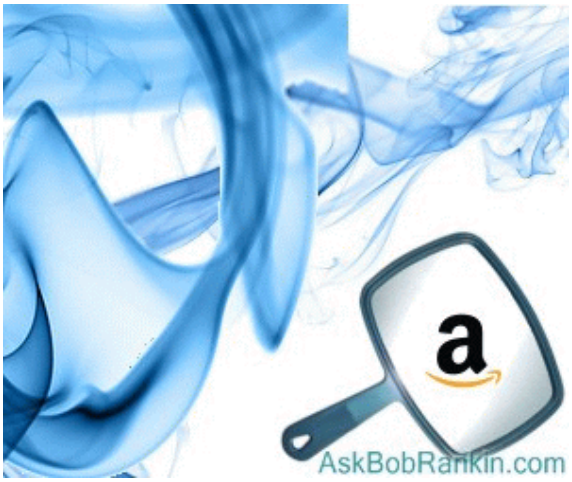
Smoke and Mirrors at Amazon .com?

by Bob Rankin
askbobrankin.com

Like millions of other consumers, I buy stuff on Amazon.com. The free two-day Prime shipping is convenient, and the prices seem to be competitive. But some eye-opening reports, a class-action lawsuit, and a new competitor are causing me to question my assumptions about Amazon. If you shop online, you'll want to read on for the details...

Has Amazon Lost Its Price Edge?

When Amazon.com debuted in 1994 (yes, 21 years ago!) it was all about low prices. The e-commerce juggernaut has relentlessly built a reputation as the first and only place consumers need to go in order to get the lowest prices. But Amazon's prices have crept upwards, creating an opportunity for new and old competitors to exploit.



Amazon Prime, with its "free shipping" and other perks, has been key to building customer loyalty and trust. But two pending lawsuits allege that Amazon betrays that trust by invisibly folding shipping charges into prices displayed only to Prime members.

An example given in one of the lawsuits says that a non-Prime shopper may see an item price of $10, plus $4 shipping, but a Prime member will see a price of $14 for the same item, with "free" shipping. Even worse, if the non-Prime shopper's order totals $35 or more, he will actually get free shipping while the Prime member pays a higher total for the same order! I've seen something similar to this myself on many occasions, where the "free shipping" is an illusion created by raising the price.

Amazon pricing: Smoke and Mirrors?

Walmart.com prices were 7% lower than Amazon.com's on a basket of 59 items compared by Kantar Retail analysts in 2014. Walmart in-store Supercenter prices were 16% cheaper than Amazon's and 8% cheaper than Walmart.com's according to the study.

Third-party sellers in the Amazon Marketplace accounted for most of the differences between Amazon and Walmart in the Kantar study. When Kantar compared "Amazon direct" grocery prices to Walmart Supercenters, it found the two were on equal footing. But household supplies were another matter, i e., Windex Antibacterial Multi-Surface Cleaner — $2.47 at Walmart Supercenter, $7.07 at Walmart.com and $9.49 in the Amazon Marketplace.

Amazon obscures its overall pricing even more by offering frequent promotional discounts and "bundles" of related products. The lack of transparency lets Amazon get away with charging higher prices overall.

I Thought The Major Was a Lady

A new challenger to Amazon's hegemony promises to eliminate the smoke-and-mirrors game. Jet.com is a membership club, like Costco. It costs $50 per year to shop at Jet, which opened in July, 2015, with over 10 million items.

A Wells Fargo analysis found that Jet.com's prices average 9% less than Amazon's on the same items. Jet.com even lists Amazon's prices side-by-side with its own on items that both e-tailers carry. Jet.com even offers to refund the $50 membership fee if a customer doesn't save at least $150 over the course of a year.

And unlike Costco, Jet.com doesn't make you buy 48 rolls of toilet paper at a time to save money. Instead, your savings increase as your total order increases. You can actually watch the prices of items in your shopping cart fall as you add more items. Orders over $35 ship for free, and they also offer free returns. The icing on the cake is an extra $10 off your first order of $35 or more.

If you're hesitant to pay $50 just to join, you can try Jet.com free for 3 months. There's no gotcha here. If you like it, join Jet and pay the membership fee. If not, you just walk away. (As of 08/28/2015, if you use the promo code CURISMA when signing up, you'll get 12 months free, instead of 3 months. I don't know if or when this code will expire.)

Jet.com is well stocked with household items such as cleaning supplies, kitchenware, home décor, etc. It's still a bit thin on electronics, sporting goods, and apparel. Perishable foods are non-existent, as is booze. (Side note: Amazon just launched two-hour liquor and wine delivery in Seattle.) But 10 million items is a good start, and with $225 million in seed money Jet.com can expand quickly.

Just as it pays to shop for car insurance once a year, it's a good idea to review your online shopping loyalties periodically. There are other options besides Amazon, and they could save you hundreds of dollars per year.

Top 10 Reasons to Upgrade to Windows 10

by Sandy Berger
COMPUkiss

If you are still on the fence about upgrading to Windows 10, it is everything that Windows 8 should have been, but wasn't. Here are 10 reasons why you should upgrade.

1. Windows 10 is a free upgrade for anyone using Windows 7 or Windows 8.1. This offer is good until July 28, 2016. After that time it will cost $119.
2. When Windows 10 starts, you are dropped immediately into the Windows 7- type desktop. Although there will be some new things to learn, end users will find that the transition to

Windows 10 will be much smoother than the transition to Windows 8.
3. Windows 10 is faster and more secure than Windows 7 or Windows 8.
4. Windows 10 is easy to use with a keyboard and mouse and just as easy to use with a touchscreen. If your computer has a touchscreen as well as a keyboard and mouse, you get the best of both worlds.
5. As a service, Windows 10 will be constantly updated to keep it more secure and more capable.
6. The new Edge web browser that comes with Windows 10 is faster and more secure than Internet Explorer. It also offers useful new features like the ability to make notes on a web page and send them to a friend and the ability to save a web page to read later.
7. Several apps like Mail and Photos have been dramatically improved.
8. Although the Start Menu is back, it is larger and more distracting than it was in Windows 7. Fortunately, it is customizable so you may want to spend some time getting it to suite your taste.
9. Cortana, a voice assistant like Apple"s Siri is built into Windows 10. You can ask her questions and she can even help you find your files.
10. The new File Explorer is much improved. It now shows a list of useful Quick Access locations and folders you use frequently in addition to Recent Places.

Everything you've ever wanted to know about eBay

Book Review: *My eBay for Seniors*

by Chris Johnson, Editor & Designer, Golden Gate Computer Society, CA

My eBay for Seniors
by Michael Miller, Que, 2014
Education, $24.99

The large sans serif type and its references to grandkids makes *My eBay for Seniors* a book geared to older folks in the publisher's eye. Everything else about the book—its information and colorful artwork—is for the beginner or average user—of any age. But I did like that I didn't have to whip out my glasses to read it.

Some of the instruction lists run into the high 20s for number of steps, but visually the book makes it seem easy with lots of clear artwork of what you"ll see on the screen each step of the way. It shows you how to buy and sell and relist items...and what happens when you make a sale.

If you want to use eBay from your smartphone or tablet, the book even has a chapter dedicated to buy and sell that way too.

Bidding for items on eBay can be exciting like in a real auction—and, except for the cost of the item (and shipping charges if additional), you pay no money to eBay to shop or buy.

When you bid on an item and a box appears on the screen to tell you that you are outbid that means that someone put in a maximum bid that they are willing to pay that is higher than the amount you just entered.

You can do the same after you are the highest bidder. The book explains how to easily set up that maximum bid up so you don't have to hover around your computer, even on the day the item's auction will end. Though eBay doesn't like bid retractions, you do have that ability under many conditions if you made a mistake.

To win an auction for an item takes a strategy. The book's 10 tips for better bidding include the recommendation to bid in odd numbers, such as $10.03 instead of $10.

The book also recommends waiting till the last 10 seconds to ever bid on anything (also called sniping) and gives a list of automated sniping services that will do it for you if you can't be up at midnight when an auction ends. One of the services listed is even free: Gixen (www.gixen.com)!

eBay also lets you keep a watch list to track items you are interested in but haven't bid on yet. The watch list is only one of many lists eBay lets you keep in your account, which is called the dashboard in "My eBay." Others include items you"ve bought or sold in the past, and more.

You can pay for items in whatever way the seller lets you pay. Oftentimes people accept credit cards, but you can almost always pay with PayPal (using your credit card or other means), which makes it even safer for you. The book even details how to set up a PayPal account and how to link it to eBay.

You can most often shop safely on eBay, but occasionally people can run across deadbeat sellers...folks who take your money and don't ship. Two chapters talks about the risks on eBay and how to minimize them.

Various colored stars for each seller is a feedback system that rates the sellers so you can know if they"ve long been trusted on eBay. Most good sellers also offer a money-back guarantee, but you"ll likely have to pay for the returning shipping costs.

Maybe you want to sell an item on eBay. The seller pays fees to eBay, not buyers. The fees depend on what the item is and how you want to sell it. The first 50 items you list each month (that's a lot!) are free to list, but you do pay a fee if it sells.

That final value fee is 10% of the total selling price (item price plus shipping/handling charges). If you are listing items in eBay Motors or Real Estate categories, the fee pricing differs.

eBay has many optional fees, such as having a boldface title, a subtitle, or a reserve price. Having a reserve price (that only you and eBay knows) lets you list an item at a low starting bid, but it won't sell unless the bidding reaches the reserve price you set in advance (you don't pay the fee, though, if the bidding doesn't reach the reserve price).

You can see the various fees at pages.ebay.com/ help/sell/fees.html. The book outlines how to use eBay's Fee Calculator too.

Another source of fees comes from PayPal, which most sellers use to receive payments for their items. Granted, eBay owns PayPal, but the fees are separate. The PayPal fee is $0.30 per transaction plus 2.9% of the amount paid to you by the buyer.

The book walks you through the process of setting up a buyer's account and the more detailed seller's account. You'll likely want to have a PayPal account too, which is easy to link to eBay. Again, the book details how to do it.

Beyond using the website, you'd need to prepare an item for sale and then ship it when it sells. The book details everything from finding items to sell to picking categories to sell it in to writing effective titles and descriptions and photographing and packing the item.

It even provides tables of grading systems for level of quality, a list of services to refer to, and the common abbreviations used, such as MIB for Mint in Box.

The book also lists what you cannot sell on eBay, such as ivory, lock-picking devices, tobacco, and used underwear...but people *do* sell them all on eBay (with cleverly couched wording in the descriptions). eBay does have an Everything Else > Adults Only category that a lot of people don't know about, but no nudity or sexually explicit content is allowed in the listing.

Although you may not copy someone else's picture for your eBay listing, you can use eBay's stock photos for certain items, such as books, CDs, and electronic products.

The book recommends that you shoot and edit your photos with 1600 pixels on the longest side (500 pixels minimum on the longest side) for the best possible display. You can post up to 12 photos for free.

The book also describes how to determine the way to sell your items: Individually or in lots? List items yourself or use a service? Sell by auction or fixed price (or both with the Buy It Now feature that lets buyers bypass the auction)?

The book really is inclusive of everything you"d want to do on eBay, from canceling an auction to blocking an unwanted buyer to packing an item for shipping. The red boxes labeled "It's not all good" gives a heads up about pitfalls to avoid each step of the way. I'm a regular eBay buyer and seller and I learned some tricks too!

AARP has teamed up with Que Publishing to help those 50+ learn how to use technology, including smartphones, tablets, computers, and social media. Que and AARP are developing new products within Que's popular "My for Seniors" book series.

The AARP community may purchase a Que book, eBook, or video today and save 40% off the list price. Use discount code AARP in the "Enter a New Discount Code" box during checkout.

RCSi Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Mark S. Lawson 544-5377
mslawson51@peoplepc.com
Sec'y: Arpad Kovacs 467-9270
podman@rochester.rr.com
Treas: Dennis P. MacMahon
taxaccuracyinc@live.com
235-1260

Board Members at Large:
Term ends 9/19:
Jan Rothfuss 544-5377
mslawson51@peoplepc.com
Term ends 9/18:
Tony Dellelo 734-6149
tonydel@techie.com
Term ends: 9/17
Bob Avery 385-4491
bobajr@sprynet.com
Term Ends 9/16:
Sally Springett 442-3776
sspringe@rochester.rr.com

Deadline for the September issue is August 11, 2015.

Planning Meeting

The meeting will be held on August 4th at 7 pm at Sally Springett's house. Everyone is welcome.

Standing Committees

Programs: . . . . . Tony Dellelo
Membership: . . . . . Steve Staub
Monitor: . . . . . Sally Springett
Webmaster: . . . . . Bob Avery
webmaster@rcsi.org
Linux SIG: . . . . . Carl Schmidtmann

unixgeek@faultline.com

Computer Recycling / Remanufacturing Center

420 Dewey Avenue Rochester, NY 14613, 2nd Floor Warehouse – behind the City Recreation Dept, Administration Building. Hours of Operation: between 9 am and 4 pm M-F (call Helpdesk first, before visiting).

Helpdesk Phone Numbers:

585-232-9160 585-719-9992

http://acdcareers.com/ Community /PCRecycling.php

Micrecycle

Computer Recycling
49 Stone St.
Amy MacCallum 224-4040
amymac@rochester.rr.com