COMPUTER NEWS from the

JULY 2014 Volume 2 NO. 7

As found on the web and other sources

Do Health Apps Endanger Privacy?

Category: Privacy
From “askbobrankin.com” on 6-10-2014

Healthcare is one of the fastest-growing industries thanks to two factors: A younger health-conscious generation enamored with gadgets, and an aging population increasingly conscious of its frailty and mortality. More and more data is being collected to improve health through smartphones, smartwatches, websites, and other connected means. But that wholesome trend also creates opportunities for data brokers to invade your privacy and sell your most intimate secrets. Here's what you need to know...

Healthy or Anonymous: Pick One

Your new smartphone is probably loaded with apps to help you monitor and improve your health. Samsung's popular Galaxy phones have the S Health app. Apple's forthcoming iOS 8 (for iPhones and iPads) is loaded with new tools to collect and store your health data.

Maybe you've got a wearable device like a Fitbit, Smart Run, or FuelBand that can wirelessly transmit information about your sleep cycles, steps taken, calories burned and heart rate. But where is all that data going?

Have you registered at a health-related Web site to obtain access to health information, track your diet, or chart your fitness levels? Have you completed a "confidential" survey to get a discount coupon? Downloaded an app that monitors your blood pressure?

No law prevents the providers of such things from selling whatever data you voluntarily give them, to marketers, insurers, and other interested parties.

Depression, herpes, yeast infections, erectile dysfunctions, and bed-wetting are just a few of the highly sensitive characteristics for which consumer mailing lists are available. Most consumers assume such things are protected against exploitation by federal and state privacy laws; they are, but in limited healthcare contexts.

Only specific healthcare "entities" are prohibited from sharing your health-related information with others. Doctors, hospitals, pharmacists, and insurance companies cannot resell what they learn about you. But a whole lot of other entities can, and they even straight-up buy it from you.

The mere fact that you visited a Web site devoted to diabetes is marketable. Sure, you may not have diabetes yourself; you may have visited the site on a friend's behalf, or as part of a research project. Such a visit, alone, won't fill your mailbox with insulin offers. But it goes into a digital dossier whose diverse bits of data form a startlingly accurate and detailed profile of your health and health interests.

Who Wants to Know?

Highly specialized lists may be purchased and combined into one huge database of people and their health-related interests. The purchasers – drug companies, medical supply distributors,

private investigators, and so on – don't rent lists based on just one criterion that may be wide of the mark. They'll specify "persons who have visited diabetes Web sites AND shopped for weight-loss products," a much more certain indication that a matching subject does have diabetes.

Ads for furniture or remodeling services may follow your visit to a site about depression. Why? Because treatment often includes advice to "change your lifestyle" and brighten up your home, and people who are recovering from depression often experience an urge to splurge on self-rewards.

Vendors of health apps and wearables say their privacy policies will keep your sensitive data safe. But the U.S. Federal Trade Commission and other privacy advocates are still concerned. The fact that any data you give to a Web site – consciously or merely by your actions – may be sold to marketers is often buried deep in voluminous privacy policies and couched in nearly incomprehensible vagaries. You should assume that any site you visit is going to squeeze every nickel it can out of whatever you do there.

"We will never sell your email address" is a meaningless promise, and it's unenforceable in the usual course of events. A site doesn't have to sell your email address; someone else did, and it's associated with your name, street address, and health-related data in several independently assembled databases. Besides, how would you know or prove that Site A sold your email address? You've left it everywhere, haven't you?

Helpful (and not so helpful) Steps to Protect Your Health Privacy

"Use a different email address" is rather useless advice even though it would help you pinpoint who sold a given address to marketers. If you used JohnDoe123@yahoo.com only on one site, then any spam sent to that address is definitely that site's fault. But how many different email addresses are you going to create?

"Actually read the entire privacy policy" is worse than useless; it wastes your time. Companies that don't plan to use your personal data for marketing purposes don't need privacy policies.

You can use cash to buy over-the-counter health items anonymously, and just say "no" if asked for any contact information. Online, you don't have much choice but to provide a shipping address, at least. But use Paypal, Square Cash, Amazon Payments, or some other payment service that does not reveal your credit card or bank account data to strangers.

"Don't over-share" on social media, especially if your posts are public by default. Discuss your visit to the doctor with friends and family via email, not on Facebook.

Finally, think long and hard before strapping a health-monitoring Internet-connected thingie to your wrist, or downloading one to your phone. You might be sharing a lot more than you assume.

Read more:
http://askbobrankin.com/do_health_apps_endanger_privacy.html#ixzz34GF3pEik

Don't forget that some of us have TV cameras attached to our computers also!
Bob

'Creepy' Facebook Feature Listens to Your Activity

By Brandon Dimmel on June, 9 2014 in "Infopackets.com".

Facebook is facing a serious backlash over a new feature that allows it to listen in on its smartphone users. When activated, the feature uses the device's microphone to detect a user's activity and automatically updates their "status" accordingly.

For example, if a user is listening to a new U2 album on their stereo in the background, Facebook will use a smartphone's microphone to update a user's status to "Listening to U2". It can also detect movies and television shows and update a user's status to read "Watching Iron Man" or "Watching Mad Men".

According to Facebook, the feature is only activated when a user is composing a status update.

Facebook Microphone Listening Feature "Downright Creepy"

This isn't the first application to use a smartphone's microphone to identify media. Shazam, an app that was released more than a decade ago, uses a microphone to show a user the artist, song title, and album of a detected song.

That said, Facebook's listening feature takes things a step further by updating a user's profile status automatically. That has led thousands of users to slam the new feature as "creepy" and a "Big Brother move". (Source: **com.au**)

Some users were so upset that they started an online petition in hopes of convincing Facebook to kill the feature. "Facebook says the feature will be used for harmless things, like identifying the song or TV show playing in the background, but by using the phone's microphone every time you write a status update, it has the ability to listen to everything," the petition reads.

"Not only is this move just downright creepy, it's also a massive threat to our privacy. The feature is opt-in, but many won't even read the warnings. If we act now, we can stop Facebook in its tracks before it has a chance to release the feature."

Those behind the petition are seeking 750,000 signatures. As of this past Monday midday, they were closing in on 600,000. (Source: **sumofus.org**)

Eavesdropping Information Anonymized, Facebook Insists

For its part, Facebook says it's easy to opt out of the program, thereby ensuring that users' information is not linked to their accounts.

"If you don't choose to post and the feature detects a match, we don't store match information except in an anonymized form that is not associated with you ... We turn the audio it hears into a code -- code that is not reversible into audio -- and then we match it against a database of code," noted Facebook spokesperson Momo Zhou.

Although the feature is clearly unpopular with a large segment of Facebook's user base, experts suggest **it could prove very lucrative in attracting marketers** and driving up Facebook's advertising revenue. (Source: **news.com.au**)

What's Your Opinion?

Do you think that the Facebook microphone listening feature is too intrusive, as the petition suggests? Or do you think concerned Facebook users should just shut the feature off and forget about it? Would you ever use or want this kind of feature on your smartphone?

Free Microsoft Security Tools

When it comes to computer and online security, Microsoft Windows is often portrayed as the problem rather than the solution. But don't get the idea that Microsoft doesn't care about security. In fact, Microsoft publishes several free and effective security tools for home and professional users. Try some of these to see if your currently installed security software is doing everything it should to protect you...

Beyond Anti-Virus:

Try These Free Microsoft Security Tools

News of security breaches frequently mention a "vulnerability in Windows." The fact is that any software is vulnerable to hacking; it just so happens that Windows is the most popular target because it's the biggest.

Are you sure your Windows system is correctly configured, has all the latest security patches, and that your anti-virus software is adequately protecting you?

Here are several free tools from Microsoft that you can use to find out.

Microsoft's Malicious Software Removal Tool scans for and removes malware after finding it. However, its signature database includes only the most prevalent threats. It would be a good idea to run Microsoft Safety Scanner (see below) after MSRT for greater assurance that you haven't missed anything.

If you use Windows Update (and you should!) there's really no need to download the MSRT, because Windows Update will do so automatically. But you can download and run it at any time if you suspect a problem.

Microsoft Safety Scanner is a good, quick way to check for known malware on your computer. It includes a malware signature database of known threats and a barebones program that searches your files for matches. Options include a quick scan of disk areas where malware is deposited most often; a full scan of entire drives; or a targeted scan of user-selected folders.

During the download, you have the option to run the tool right away, or save it to a flash drive or CD for use on another computer. To ensure that you use the most recent malware signature database, MSS expires every ten days and must be downloaded again. Because it's a rather large download (over 90MB), I recommend using Microsoft Safety Scanner only if you suspect that your existing anti-malware program has failed to catch or remove a problem. It can also be run every few months to double-check your antimalware program's effectiveness.

The Microsoft Malware Prevention Troubleshooter goes by the short name, “FixIt.” This utility turns on Windows Firewall; Automatic Update (so you automatically receive and install critical security updates); Pop-Up Blocker in Internet Explorer; and User Account Control. Note that many users disable some or all of these features deliberately, either relying on third-party firewalls and other protections or simply preferring not to be bothered by UAC.

FixIt also enables features that check for active anti-malware software and nag you if you don’t have any installed; stops the Remote Registry service if it is active, preventing hackers from modifying your registry settings; monitors Internet Explorer to make sure it is up to date and privacy/security settings are tight; and resets your proxy settings to ensure a normal browsing experience if malicious software has hijacked them.

The Enhanced Mitigation Experience Toolkit makes malware’s attacks more difficult by protecting certain operating system features that must be circumvented before vulnerabilities in Windows can be exploited. It will also "harden" the defenses of certain programs that are commonly used as attack vectors, such as Internet Explorer, Microsoft Office, Adobe Reader and Java.

In addition, it tightens the rules for verifying the identity of popular online services such as Twitter, Facebook and Yahoo. EMET supports Windows 7 or 8, Windows Vista, Windows Server 2003, and the Home or Premium edition of Windows XP.

Microsoft Baseline Security Analyzer scans local and remote computers to see if they have the latest Microsoft security updates for Windows or MS Office and whether there are any security misconfigurations that leave the door open for malware or hacking. Some things the MBSA looks for are missing security updates, weak account passwords, and misconfigured firewalls.

The Microsoft website says the MBSA is a tool for IT professionals and system administrators, but don't let that scare you away. If you're a typical home computer user, then you ARE the system administrator. You will need to know in advance if you have a 32-bit or 64-bit version of Windows, and then select the corresponding download. Note that the program doesn't automatically run after the download. You'll need to find the downloaded program and then launch MBSA. After it runs, MBSA will display a report of any problems found, with links to remedy them.

Windows Defender Offline is a tool that's fundamentally different from all of the ones I've mentioned here so far. The difference is that it doesn't run while Windows is active. it's a standalone program that runs from a bootable disk. WDO will boot up a bare-bones environment in which neither the Windows operating system nor viruses can activate. It then scans your hard drive for malware, and will remove any if found.

If your system is so badly fouled up that you can't even download or run a malware scanner, or if you cannot boot Windows because of a malware infection, then WDO is a handy tool to get back to good.

What About My AntiVirus Program?

To be clear, I'm not recommending that you use any of these tools instead of your current anti-virus program. Consider the tools listed here as an extra layer of defense against malware. Use them as a "peace of mind" scan to check for cyber-nasties that can sometimes creep in undetected.

No anti-virus program is going to protect against 100% of all threats 100% of the time. The reason for this is that new viruses are being created all the time, and viruses can morph (change their identifying characteristics) and attack before your antivirus program is updated. It's also possible in some cases for a virus to disable your antivirus protection.

I'm sure many people reading this will be wondering why I didn't mention the obvious -- Microsoft's free Microsoft Security Essentials antivirus program. The short answer is that I don't recommend it. The long answer is in my article Microsoft Security Essentials: EPIC FAIL.

For a list of free antivirus software that I do recommend, see my article Free Anti-Virus Programs.

Read more: http://askbobrankin.com/free_microsoft_security_tools.html#ixzz33hPhhrX8

WHAT THE !@#%&^*(*&

No More Free Antivirus?

I have noticed an increase in puzzled, indignant emails from readers asking why I say antivirus programs are free when they aren't. Typically, the writer says he/she downloaded the 'free' program and has been using it happily for anywhere from a month to a year, but suddenly the program says it's time to 'upgrade' and that's going to cost money. I'd like to clear the air on what's happening here...

Which Antivirus Software is Really Free?

Virtually all antivirus software developers offer two or more versions of their wares. The version that I say is "free" is truly free, perpetually – for personal, non-commercial use. If you've run into a situation where you downloaded what you thought was a free antivirus program, and it seems to asking you to pay, read on...

The confusion arises when users make a wrong turn by mistakenly download the "trial" version of an antivirus program. Trial versions, generally, are fully-functional but only for a limited amount of time. You get to try it before you decide whether to buy it or stop using it. But the language and layout of the download pages can be confusing, if you're not paying close attention. Let's look at three of the most popular antivirus freebies:

On the AVG download page, the column on the left says "Free Download" and that's the freebie. The column on the right says "Free Trial". If you download that one, you'll most certainly get a nag screen after a period of time asking you to pay for the product. On the Avast download page, there's a similar, but slightly more obtuse situation. There are three columns, all labelled

"DOWNLOAD" but only the leftmost button will get you the freebie. Avira gets kudos for making the link to the free download most abundantly clear.

But even if you succeed in getting the truly free version of your chosen anti-virus software, you might hit a bump in the road later on.

Consumer confusion is increased by many software developers who want to eat and pay their employees. When a new updated version of a program becomes available, it is often presented to users along with a sales pitch to "Register", "Renew", "Upgrade" or some similar language that seems to indicate that money must be paid. But somewhere, perhaps down at the bottom of the screen, you will find a button or link to “stick with the free version.”

I recently got a popup from Avast that said something like "Your avast! protection will expire soon - RENEWAL REQUIRED." A careful reading of that screen indicated that I could continue using my free version by registering it, at no charge. But I can see how many are scared into thinking that they must upgrade to the paid version.

For more information on free antivirus software, and other internet security tips, see my article Free AntiVirus Programs.

Offers to “Upgrade to Pro” are scattered all over most free versions of antivirus software on the control panel’s main screen; in the “settings” and “maintenance” areas; and in the “about” and “preferences” areas. Essentially, they are ads in this “ad-free” free software. They’re just not ads for other products.

So always-free antivirus software is still available, and I will not call a program “free” unless it is. But you have to read the developers’ offers mindfully to make sure you get what you want to pay (or not pay) for.

Paid versus Free Versions

My current favorite, Avast Free Antivirus includes basic antivirus, anti-rootkit, and anti-spyware protection. Other versions, which are available on a trial basis, add more and more features such as a firewall, anti-phishing and anti-spam defenses, and a “SafeZone” feature that creates a virtual machine in RAM every time you log in to a bank, e-commerce site, or other site where security of the data stored on your real machine is essential. The virtual machine is “clean” of all personal data, and anything that a Web site might inject into it during a session vanishes along with the virtual machine when the session ends. (See also Why I Switched from AVG to Avast Antivirus.)

Avira Free Antivirus includes everything a typical non-commercial user needs: excellent off-line scanning and removal of infections; real-time protection against drive-by downloads and phishing threats; blocking of attempts to track your Web activity or infect your system with spyware or adware; and a reputation-based rating system that warns you if a Web site you’re about to visit is suspicious.

The paid versions – three "suites" – include the features above and add others that may be of critical use to personal or business users. For instance, the free version of Avira does not scan email for viruses but the suites do. Is that important to you? If you use an email service provider that scans for viruses before delivering mail to you, probably not. If you are running your own mail server with no antivirus, or use a third-party provider who doesn't scan for viruses, you do need one of the Avira suites.

AVG Antivirus devotes a large part of its Wikipedia entry's "Products" section to the limitations of the Free edition. The most noteworthy limitations for personal, non-commercial users are: 1) no rootkit protection; 2) infrequent updates; and 3) no phone or email support. (No other vendor offers one-on-one support to free users, either). Also, the Free edition displays a popup ad for upgrades to the "Internet Security" paid versions every day for one month per year. Each year, you have to re-confirm your free registration, at which time you will get a heavy sales pitch to buy an upgrade.

Comparing the features of free vs. paid versions of antivirus software is more confusing than comparing cellular phone service plans. Developers use code words like "SafeZone" without providing ready access to a definition (I had to Google it). But it sure sounds like something you absolutely need. The idea is to offer a free version but give the user the definite impression that he'd be better off paying. If you have a computer that's shared with kids, or someone who is hell-bent on clicking anything and everything, it's probably a good idea to go with a paid product for the extra protection offered.

Whether you decide to pay or not depends, to a large extent, on whether you have actually experienced a problem that a paid version of the software can prevent. Until then, you don't know the full pain of the problem and so you don't feel the need to spend that money. You may also want to thank the developers after using the free product for a while, by purchasing a paid upgrade. I've always done well with the free security tools, but the choice is yours.

Your thoughts on this topic are welcome. Post your comment or question below...

Read more: http://askbobrankin.com/no_more_free_antivirus.html#ixzz35E3cK4Im

---

A little humor to end this news letter:

IF A PARSLEY FARMER IS SUED, CAN THEY GARNISH HIS WAGES?

WOULD A FLY WITHOUT WINGS BE CALLED A WALK?
